
# National Cybersecurity Strategies: Review and Analysis of Evaluation Frameworks

University of Oulu
Information Processing Science
Master's Thesis
Juha Haaga
7.6.2021

# Abstract

National cybersecurity strategies (NCSS) are becoming increasingly important for society. They provide essential support for the development of both digital and traditional infrastructure, and a well-designed strategy can have a tremendous positive impact on a country. Therefore, for developers of a new strategy or researchers of previously published ones, it is good to understand the current state of the art on evaluating national cybersecurity strategy documents. Unfortunately, while there is some research on these strategies and comparisons between them, the published work is superficial. Moreover, the publications do not disclose their research methods, so it is challenging to evaluate their results. These limitations make it difficult to rely on previous research.

Objectives and proposed activities to achieve the desired outcomes form an essential part of a national cybersecurity strategy. However, little research on them exists. The relevant NCSS guides focus on structuring the entire drafting process at a high level, without details or suggestions on subtopics such as typical objectives or activities. This thesis addresses the research question: How are activities and objectives defined in the evaluation frameworks, and how do they relate to each other? In particular, can they be analyzed in a replicable way so that a body of knowledge of common and valuable objectives and activities in NCSS could be built?

It turns out that the existing definitions for objectives are lax. There is no consensus between NCSS writers or researchers in this domain on defining an objective or activity. As a result, these are readily mixed in the source documents, and the analytical frameworks that were studied are not extracting them reliably from the source documents.

The constructive analysis is one way of consistently defining the objectives and activities and applying a practical inference method to discover the connections between them. This approach was tested with the source material available from the previous works.

By applying the method in this research, objectives, and activities were classified more rigorously. The classification work enabled a better understanding of the activities and further analysis of their relationships, which were then documented and organized into a graph representation. That graph of objectives and activities can help readers and developers of future strategies to think about how to organize the goals of their NCSS. Furthermore, this research could provide a way for systematically expanding the body of knowledge about the requirements and dependencies, thus making it more straightforward to include objectives and activities in future strategies.

Finally, several future research avenues are discussed, which would expand the knowledge about the NCSS documents and begin to track their evolution more robustly over time. For example, there are avenues for both manual analysis and machine-learning-based unsupervised learning methods that could be applied for further insights.

*Keywords*
National Cybersecurity Strategy, analysis framework review, cybersecurity objectives, cybersecurity activities, conceptual analysis, constructive analysis

*Supervisor*
Professor Jouni Markkula

# Foreword

I wish to thank my mother, Kaarina, who passed away before my graduation, but always insisted that I should return to the university and finish my degree, despite already having been employed in the cybersecurity field for a decade.

I am grateful for the continued support of my thesis advisor, Professor Jouni Markkula, for his invaluable help in organizing my thoughts about the thesis topic and for ideas about different research methodologies that could be applied. In addition, I would like to thank him for his patience when this thesis took a longer time to be completed than initially planned.

Working on this thesis was enjoyable from the beginning and helped me immensely on my path to become a cybersecurity professional. During the project, I met many interesting people in this field and exchanged ideas about cybersecurity strategy in general.

I hope that the completed work finds some interested readers as well, to help you along in your journey, as it did for me.

Juha Haaga

Espoo, June 2021

# Contents

# 1. Introduction

Cybersecurity is a discipline needed to prepare us properly for the current and future challenges of the information systems-based society. Information technology has become woven into every aspect of our lives and promises a staggering amount of new opportunities. However, in a world where many actors do not have our best interests in mind, cybersecurity is necessary to secure the environment where people, government, and companies interact in this new environment (Lehto, 2013.)

Making that environment secure will help us reach the potential economic development resulting from the information-based society while countering some risks to personal privacy, commercial predictability, and national security. Moreover, cybersecurity generates trust and confidence, which enables prospering digital economy. (Teoh and Ahmad, 2017.)

Government is responsible for protecting the safety of the citizens in the cyber domain at the country level. Every country is different, so by necessity, they will have varying objectives in cybersecurity. One country aims to increase the baseline cybersecurity capabilities; another country may be realigning its already significant capabilities to reap economic benefits. They may also have agenda of exerting the maximum influence on other countries in the cyber domain.

A national cybersecurity strategy is significantly different from a cybersecurity strategy of an organization. An organizational cybersecurity strategy aims to secure a bounded system against disturbances that can damage the business, viability, or reputation. There are guides for creating this kind of organizational strategy (Woody and Ellison, 2020), but these guides are not applicable for devising a national cybersecurity strategy.

The purpose of the national cybersecurity strategy is to set the vision and objectives to be accomplished, define the domain to be secured, divide the responsibilities for activities to the different authorities, and put the short and long-term goals and priorities for those participating in the effort. It sets out what approach and means will be used to reach those goals, and it may also define the timeframe for completing the improvements. As the size of government investment into cybersecurity for individual countries grows into billions annually (Network Security, 2016), having the state's resources aligned to achieve those goals is crucial.

The national cybersecurity strategy (NCSS) is also a governmental communications tool to improve the national information infrastructure's resiliency. It aligns all the stakeholders' vision and communicates the grand project's objectives and activities. An excellent strategy document includes definitions of how the success of its implementation will be measured and when it needs to be updated. Updating the strategy to match with the environment is necessary for it to remain relevant for the government.

Europe is one of the world's most progressive regions, based on the number of published NCSS documents by the EU member states and publication date for the first versions. At the time of writing, all 27 EU member countries have published such a document. In addition, the European Union Agency for Network and Information Security (ENISA) has been guiding and providing resources for EU member states for some years to set up effective NCSS. For example, the Good Practice Guide on NCSS (Falessi, Gavrila, Klejnstrup, & Moulinos, 2012) and an evaluation Framework for NCSS (Robinson, Horvath, van der Meulen, Harte, & van der Sar, 2014.)

Despite the internet having been quite central to most people's everyday activities since the early 2000s, cybersecurity policy is still a topic where only the more forward-looking countries have extended experience. Very few of the NCSS documents are beyond their second editions. In Europe, only five countries have published three editions of their cybersecurity strategy: Finland, Estonia, Germany, Greece, and Luxembourg. Many countries are still implementing their first versions, which typically have 4 to 6-year lifetimes. (Enescu, 2020.)

There is limited experience in crafting cybersecurity policies. At this phase of the NCSS document availability, the community writing them is still striving to establish a good enough foundation for building the future iterations of their NCSS documents. Efforts and guidance to this end have now been spearheaded by International Telecommunications Union (ITU) and the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford.

According to a listing compiled at CIPedia.eu (Luiijf, 2019), 104 nations have, as of Feb 2021, published one or more NCSS document versions. That means just about half of all countries have done so. The publication pace is steadily increasing as others seek to catch up with those with a strategy for national cybersecurity.

Research into cyber security strategies makes them more effective and robust and ensures a better fit in the practical and political situation in which they are published. In addition, documenting the common NCSS objectives and their requirements and dependencies informs the preparatory studies and evaluations of previous strategies that precede the new iteration of the strategy. While countries have varying starting points, there are not dramatically different desired outcomes, and infrastructure and citizens are protected in the same way regardless of the continent. In the end, cyber security in one country is quite similar to another. The differences are about where they are starting and where they want to arrive in a few years. Therefore, academics have great potential to help the government officials tasked with developing the strategies.

As more NCSS documents are becoming available for analysis, it is possible to study how they are typically structured. Analyzing many of them can also help answer the question, "what should they contain?" Results from these analyses are helpful for those who need to write NCSS documents of their own. There is a tremendous amount of duplicated work in cybersecurity strategy development when experts in each country come up with the objectives and evaluate how practical those are to reach within the available means and time. Additionally, the availability of supporting research makes the strategies easier to write.

Even though cyber security strategies are essential in modern society, there appears to be very little existing research on how well the strategies work and how they could be improved. The supporting material available for the practitioners barely extends beyond guides written by various interest organizations. The majority of academically published research typically restricts their scope to either describing the process of how a particular strategy was developed or to comparisons of strategies in pairs. The most extensive comprehensive analysis of NCSS documents extends to 19 documents, and the results of it turned out to be challenging to trace back to the source material. From the information processing science viewpoint, these strategies can also be evaluated using automated machine learning-based algorithms, but the applicability of that research is still an open question.

Regardless of the above, the analyses are helpful source material to study how the various existing NCSS documents relate to each other and observe what commonalities exist. Each existing analysis of multiple strategies naturally has a different viewpoint and approach, and consequently, produces somewhat different results from the others.

This thesis identified some of the differences in the approaches used to analyze the NCSS documents and looks for ways to improve the strategies. Comparative and lexical analysis-based studies are appropriate for this field because the available data used in the existing analyses have not been enough for in-depth statistical analysis. However, that kind of study will become feasible once studies incorporate most of the current strategies into their scope and the number of available NCSS documents increases. In addition, the methodologies that were used in the previous studies were not documented, so using the lexical analysis applied in this work can provide a more rigorous starting point.

The primary research question was: *What is the current state of evaluating national cybersecurity documents?*

Research into the NCSS evaluation frameworks also made it apparent that there was a fascinating disconnect between the results of the existing evaluation frameworks when it came to the definition of activities extracted from the NCSS documents. The results of the current studies were compared to sample strategies to identify how closely they were associated with the source material. The topic of object/activity definitions is of particular interest. Observations about the activities as listed in the evaluation frameworks lead to additional research questions:

*How are activities and objectives defined in the evaluation frameworks, and how do they relate to each other?*

There is very little published guidance on this area of cybersecurity objective and activities definitions, generally limited to a few paragraphs of high-level commentary on the NCSS guidance documents. Better definitions for these objectives in certain areas are identified by analyzing objectives listed in the evaluation frameworks, with the aim that future document analyses adopting these improvements would produce more consistent results and so that those analyses could be more readily replicated.

To properly study the results of various analyses, one needs to assess the results from a valuable perspective for the community. NCSS documents usually target multiple audiences, such as other parties within the government, the private sector, and individual citizens. Any of these would be suitable choices from the analysis perspective. However, the governmental perspective of the future writers and policy-makers of NCSS strategies was chosen because it can help push this field forward. This thesis will consider the objectives and activities one can define in the NCSS, based on the previous research, and strive to document their relationships.

This thesis aims to help the reader understand how commonly defined activities in NCSS documents relate to each other, how they have been investigated and compared in the past, and how they could be further studied. The results also provide insights into what kind of analyses are possible and feasible.

The research material for the thesis was selected in the literature review phase primarily based on how many NCSS documents we studied in the analysis. Differences in the selected evaluations were compared to each other, and shared parts of the topic grouping work done in the earlier research were investigated. Interesting perspective differences

were discovered in how researchers approached the topic groupings. However, there is no apparent consensus on how the objectives and activities of NCSS documents are defined were found in the research frameworks.

The content of one of the NCSS document analyses that included an extensive list of extracted objectives and activities was investigated by using constructive analysis. Then, the content from the study was further refined by the categorization into objectives and activities. The categorization was performed by applying the practical inference method with reasonable success. The resulting categorization was then compared to the available source material to validate the research method.

Following the categorization, links between the activities were studied, and the linked activities are mapped to a graph format. The activities were then further analyzed to discover the level of abstraction and connections between them. Abstraction level was found by applying a topological sorting method on the graph of discovered activities by their connections. Describing the discovered activities in a meaningful way sorted by their dependencies is one of the thesis's primary contributions. Furthermore, it offers a practical way to discover valuable information for developing future cybersecurity strategies.

The research also shows that several potential novel approaches for further research would appear to be feasible. The source material has diversified and improved significantly since the previous comprehensive analysis was performed and is past due for a new analysis. Besides different kinds of manual research, the domain is now a good candidate for additional machine learning-based approaches. A few different lines of inquiry discussed at the end offer new ways to advance research into this topic of NCSS document analysis.

# 2. Prior research on national cybersecurity strategies

Relevant research into cybersecurity strategies can be classified into a few categories. First, research establishes the function of cybersecurity strategies and provides some guidelines on how to write one, and then there is research analyzing existing strategies. However, before getting into them, defining what we mean with cybersecurity and cybersecurity strategies is essential to establish what we are trying to improve.

## 2.1 Cybersecurity and strategy

Cybersecurity is a term with a wide variety of definitions. Some definitions are very narrow and describe what used to be known as information security, while other definitions are expansive. Some include everything related to the information infrastructure and assets and then expand to encompass how people in the information era interact with that infrastructure and how information security affects society.

International Telecommunications Union (ITU) offers the following definition:

*"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment"* (International Telecommunications Union, 2019.)

The above definition by ITU is somewhere in the more expansive end of the spectrum as it includes more terms and areas of focus. Their definition would be well aligned with the study of national cybersecurity strategies that share that perspective.

There have been attempts to define cybersecurity's meaning by a commonality analysis of definitions extracted from multiple sources (Schatz, Bashroush, & Wall, 2017). Using this approach, the definition that most closely matches that consensus view is the first part of the definition offered in the NCSS document of South Africa and the first sentence of ITU's definition. Therefore, that could be considered to be a de facto standard definition.

Von Solms (2013) has argued that the difference between information security and cybersecurity is precisely this expansion of concern from protecting information to protecting the people who use those information systems. For example, he presents cyber home automation and cyber terrorism scenarios as cases where the damage is to society's physical assets and order. Politically motivated influence cyber operations (ICO) have become much more prominent in the last few years and provide another excellent example of cybersecurity concerns that transcend information security. Brangetto and Veenendaal list different kinds of operations included in the ICO category. The operations mix information infrastructure-related attacks with attacks that target persons and institutions, such as doxing. (Brangetto and Veenendaal, 2016.)

As is the case with the definition of cybersecurity itself, cybersecurity strategies likewise do not have an established or commonly accepted definition. That, of course, does not mean that there are no definitions, and several parties have attempted to offer one, such as Azmi et. al:

*"a careful plan or method of protection both informational and non-informational assets through the ICT infrastructure for achieving a particular national goals usually over a long period of time"* (Azmi, Tibben, & Khin, 2016, s. 2).

ITU does not provide a single sentence definition in the NCSS development guide but instead offers a list of ways to think about the cybersecurity strategy:

- *An expression of the vision, high-level objectives, principles, and priorities that guide a country in addressing cybersecurity;*
- *An overview of the stakeholders tasked with improving the cybersecurity of the nation and their respective roles and responsibilities; and*
- *A description of the steps, programmes, and initiatives that a country will undertake to protect its national cyber-infrastructure and, in the process, increase its security and resilience.*

(International Telecommunications Union, 2018, s. 13.)

These guidelines are helpful. In the ITU definition, it is noteworthy how the high-level objectives are mentioned separately from the steps and initiatives necessary to understand what will be done.

The definition of cybersecurity strategy can also be looked at from the perspective of the motivation that countries offer for presenting one. Azmi explains ten motivations that can be further grouped into three main categories: national security, jurisprudence, and politics. (Azmi et al., 2016.)

When it comes to the contents of national cybersecurity strategy documents, a distinction can be observed between documents that mix strategy and implementation into a single document and approaches where those are separated into two separate documents.

## 2.2 Cybersecurity strategy evaluation frameworks

This section discusses the related research on the National Cybersecurity Strategies and the existing evaluation frameworks used to study the strategy documents that were selected as primary sources.

After reviewing the literature, there are four primary sources to consider when reviewing NCSS documents and evaluations. Three sources are analyses of NCSS documents that review, summarize and manually categorize a significant number of documents (10-19). The fourth analysis attempts to use clustering and topic modeling methods to discover what topics may exist in the more extensive set of sixty NCSS documents. Each of these approaches provides different kinds of insight into what NCSS documents typically have in common.

Luiijf et al. have, in their work, analyzed and compared 19 different NCSS documents worldwide (Luiijf, Besseling, & De Graaf, 2013). The research paper included as a primary source is an expanded work based on his earlier analysis of 10 NCSS documents in 2011 (Luiijf, Besseling, Spoelstra, & de Graaf, 2011). Thus, the second publication can

be considered to supersede the original. Their study does not explicitly set out to develop a framework for evaluating the documents in the future. Instead, it documents the result of applying a comparative study technique into several NCSS documents.

When discussing the comparison results, Luiijf describes an ideal NCSS document based on a standard set of features identified from the research material. Luiijf's proposition for an ideal structure provides a valuable template, and it is a good candidate for comparison to other frameworks (Luiijf et al., 2013). However, given that no other works propose a structure for an NCSS document, there is no existing review of this part of their study.

ENISA has published an evaluation framework for analyzing NCSS documents. The framework was developed by analyzing existing NCSS documents, complemented by a literature review. The model that ENISA produced consists of a logic model for describing the content and structure and a set of possible Key Performance Indicators (KPI) for tracking the performance of the document. The NCSS evaluation framework published by ENISA (Robinson et al., 2014) developed by the EU Cybersecurity authorities to aid the EU member states in their work serves as a primary source.

In addition to presenting the framework, the authors also discuss the results of studying several European NCSS documents and the frameworks used to compose them. Additionally, in the ENISA study, the authors performed a survey of national cybersecurity authorities to extract additional information about their respective national strategies. They also interviewed public sector stakeholders to get a better overview of the domain. Finally, since the studied NCSS documents did not apply a systematic program-level evaluation framework, the authors also created one for this scenario.

The third primary source is a report produced by the OECD that analyzed existing NCSS documents and collected data from governmental cybersecurity strategy decision-makers. OECD analysis differs from the work of Luiijf in that they did not rely exclusively on the information that was printed in the NCSS documents but instead composed a set of questions that an appropriate authority in the 10 OECD member countries responded to then used that information in their analysis. Moreover, unlike in the analysis of ENISA, they did not directly interview any experts. (Bernat et al., 2012.)

The clustering algorithm-based approach attempted by Kolini et al. provides an interesting perspective into this research because it sidesteps the inherent human grouping biases for the documents and relies on the frequency of relevant words to extract a set of topics sharing certain similarities from the source material. Human evaluation is then applied to describe the machine-generated topics and assign them meaning based on the context found in the analyzed documents (Kolini and Janczewski, 2017.)

There are also several other attempts at analyzing the NCSS documents besides the three mentioned above. For example, Min has studied an NCSS document's essential features (Min, Chai, & Han, 2015), while Shafqat has defined a helpful set of metrics for analyzing the documents (Shafqat and Massod, 2016).

Also, Lehto has analyzed the high-level structure of NCSS documents and identified which sections have the most commonalities and which sections have the most considerable variance between different documents (Lehto, 2013). Additionally, there is an analysis comparing NCSS documents in EU and NATO contexts, but it is limited to analyzing high-level commonalities and differences (Štitilis, Pakutinskas, & Malinauskate, 2017).

These approaches would be suitable for complementing the detailed analysis performed in the four primary sources. However, they do not extract a sufficient amount of material from the source documents in the way that the primary sources do, which sets them apart.

## 2.3 The aim of the NCSS document

Although this study's focus is to understand how NCSS documents have been analyzed and understand the activities defined in the NCSS documents, it is beneficial to understand these documents' purpose better. Their purpose can describe the aims and priorities needed for a nation to develop in a positive direction in cybersecurity. NCSS document needs to set forth these priorities straightforwardly, making it easy for the implementers to work towards them and align with each other.

Luiijf identifies three general aims for the NCSS document (Luiijf, 2013, pp. 4-5):

- *Aligning the government*
- *Coordinating the focus, roles, and responsibilities of the various stakeholders*
- *Conveying the national intent to other nations and stakeholders*

The ENISA guide proposes the aim of the strategy as follows: *"The aim of a cybersecurity strategy is to increase the global resilience and security of national ICT assets, which support critical functions of the state or of the society as a whole."* (Robinson et al., 2014, p. 8)

The definitions are similar, but in the ENISA version, the communications function is left out. The omission is interesting, as one of the ENISAs main functions is to communicate strategic advice to the European member states. One would think that the emphasis would be reflected in their publications.

## 2.4 Ideal contents of an NCSS

In their comparative study of 19 different NCSS documents (Luiijf et al., 2013), Luiijf also proposes a structure for an NCSS document to effectively communicate the vision and the common goals of such strategy. Clear communication is essential to the authorities tasked with implementing the plan and the citizens that the strategy was intended to protect. Moreover, Luiijf argues that following a predefined structure would also help each country avoid omitting any crucial details in a strategy.

The proposed structure is as follows:

1. *Executive Summary.*
2. *Introduction.*
3. *Strategic national vision on cybersecurity.*
4. *Relationship of the NCSS with other strategies, both national and international, and existing. [sic]*
5. *Guidance principles.*
6. *Relationship with other strategies, both national and international, and existing legal frameworks.*
7. *Cybersecurity objective(s), preferably one to four.*
8. *Outline of the tactical action lines.*
9. *Glossary preferably based on an international harmonized set of actions.*
10. *[Optional] Annex. Envisioned operational activities defined in a SMART way.*

(Luiijf et al., 2013)

The 4th point in the proposed ideal structure seems identical to the 6th and includes a printing mistake. The mistaken duplication was confirmed in correspondence by the author, and there was no 4th point that had been omitted. With these changes, the result is a list of eight required sections and one optional.

There is also further research on developing the ideal contents in the guides published by GCSCC (Global Cyber Security Capacity Centre, 2016) and ITU (International Telecommunications Union, 2018). In addition, other researchers have studied this in the context of their country's national efforts to discover the best way to define their first or second versions of the NCSS documents. For example, research has been published in the context of one of the EU countries with highly developed IT infrastructure in Lithuania (Štitilis, Pakutinskas, Laurinaitis, & Malinauskaitė-van de Castel, 2017), or in the context of a country in a developing region in South Africa (Ellefsen, 2014).

## 2.5 Cybersecurity capability maturity model for nations

The Global Cyber Security Capacity Centre (GCSCC) at Oxford University has developed a Capability Maturity Model-based approach for understanding the current capabilities of nations. The GCSCC dimension model's research is interesting because it allows repeatable measurement of how existing strategies fit into their structure. The current model is in its second iteration, and it had been applied in 2017 to study the maturity level of more than 60 countries (Global Cyber Security Capacity Centre, 2016).

The GCSCC publication contributes to this study by providing another reference set of capabilities in the five different dimensions that they chose to measure to rate the country's capability. These capabilities can be compared with the other discovered frameworks to identify commonalities. Since the five dimensions are broken down into 26 subitems, it also presents an interesting reference point for both OECD and Luiijf's analysis of the activities. Many capabilities are the results of objectives and the associated activities defined in NCSS documents. The capabilities that exist can be independent of the strategy, developed organically over time by various stakeholders before the strategy itself was formulated. The GCSCC framework is practical in establishing the current level of capability is. (Global Cyber Security Capacity Centre, 2016)

# 3. Research method

The thesis started as a review of selected cybersecurity evaluation frameworks and was then expanded to cover the activity analysis. The goal was to find answers to the research questions:

- How have national cybersecurity documents been evaluated?
    a. How do the evaluation frameworks compare with each other?
    b. How are activities and objectives defined in the evaluation frameworks?
- How do the discovered activities relate to each other?

There was a need for several different analytical approaches to dig into the research questions, work with and extract relationships with the conceptual analysis method from the activities and objectives, and then analyze their relationships using a relationship graph and topological sorting.

The existing frameworks were studied by comparing them to each other. The comparison was made by looking systematically at the different steps identified by each of the frameworks and comparing them to see where they differ or if the other framework omitted that step. This work is presented in chapter 4 of the thesis.

## 3.1 Evaluation framework selection criteria

Since this thesis is a review of a set of research projects that attempt to analyze NCSS documents using various research methods, it needs to have selection criteria for the papers that perform NCSS document analysis. The first criteria for source selection is the depth of the material studied in the publication. The research should have analyzed several strategy documents to have enough content to be beneficial compared to other analyses. In practice, research where analysis of fewer than three documents was done – such as comparing two NCSS documents – is not sufficient for it to be included as a primary source.

The NCSS documents that the research analyses should be from countries with published official documents on the matter. Preliminary studies on unpublished NCSS documents did not meet the selection criteria. For example, numerous research publications describe the methodology and approach that a country uses to define its upcoming NCSS. These are not yet published NCSS documents and, as such, could not be included as material in this thesis.

Search for the evaluation frameworks was conducted in online publication databases using keywords such as “cybersecurity strategy,” “national cybersecurity strategy,” and their spelling variations. An online search using a website search engine was also done to discover work published through various cybersecurity-related agencies. ENISA’s work was found in this way. The search was done only for studies published in the English language. Four published studies matched the selection criteria for a primary source after surveying the available literature for candidates and removing studies that did not cover a sufficient amount of NCSS documents.

**Table 1:** Relevant primary sources for the review

| Source | Author |
|---|---|
| Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy | (Bernat et al., 2012) |
| An evaluation Framework for National Cyber Security Strategies | (Robinson et al., 2014) |
| Clustering and Topic Modelling: A New Approach for Analysis of National Cyber Security Strategies | (Kolini and Janczewski, 2017) |
| Nineteen National Cyber Security Strategies | (Luiijf et al., 2013) |

## 3.2 Comparison of the existing frameworks

Two different comparison methods were used to look at the differences between the analysis frameworks. The frameworks can be divided into two categories. First, three of them analyze the structure and intents of NCSS documents (Luiijf, ENISA, OECD) and propose ways to write a better NCSS. Second, two of them analyze objectives and activities (Luiijf and Kolini) and make conclusions about them.

The first type of documents was reviewed by comparing the sections present and omitted and observing their differences. In addition, differences between approaches were noted, and they were also compared to observations from other related research material.

The second set of analyses was studied and compared to each other based on the objectives and activities they reported to have found and which grouping or topics they proposed. These were then compared to each other to see if their findings could be validated in some way.

## 3.3 Conceptual Analysis

Previously published research in NCSS document analysis had not disclosed, or at least not published, their internal methodology on how the activity was defined. The lack of description of the previous research methods was an obstacle for comparing the defined activities in each analysis. As a result, it became necessary to arrive at a formal definition of activity while analyzing the NCSS related activities identified in the source material. With the definition at hand, they could be readily analyzed and compared to the results from other documents.

One way to create such a definition is by using a conceptual analysis method. Conceptual analysis can be performed using three methods: constructive analysis, detection analysis, and reductive analysis. From these three methods, constructive analysis is used when the relations in the language terms studied are not explicit. Its purpose is to make those relations explicit. Kosterec provides a methodology for devising a model for analyzing the activities using the tools that constructive conceptual analysis provides. (Kosterec, 2016.)

### 3.3.1 Constructive analysis methodology

The constructive analysis method described by Kosterec includes six sequential steps that should be followed to apply the method. This chapter describes how those steps are applicable and were applied in the research method adopted for this thesis.

*1. Specify the initial conceptual background, CB!*

The method was applied in the context of analyzing activities discovered in the NCSS documents. Frameworks analyzed did not posit any relationships between the activities; they were taken as-is from the source documents. The activities were also given without background information on how they were chosen.

*2. Formulate the conceptual problem, P!*

Activities compose a more extensive set of tasks that need to be achieved for realizing a cyber secure country, and it is assumed that those tasks must be related to each other in some yet undefined way. Thus, there may be more than one relationship, and the same relationships may not apply to all the activities.

The set of activities to be analyzed is not complete; many activities could be added, but the operative set comprises the activities discovered from the studied NCSS documents. In addition, there is no guarantee that all the activities are related to each other directly; the set may relate to each other through a third activity that is not defined and may not have been included in the set.

On investigation, there did not appear to be existing literature that would explain these relationships. However, there may be documents that provide those activities in a context that could establish some relationship between them. Delving into the context present in the source documents was beyond the scope of this research.

*3. State the new conceptual relation R!*

What was interesting for this thesis is the relation: is activity A related to activity B. We also seek to identify the prerequisites of the relation: which activity is required for another activity?

If sorted in this way, what can be said about the activities? Later, we also seek to establish the level of abstraction but can only do so only in the activities' context. Because the level of abstraction is only established within the set of activities, the ability to do it is contingent on first establishing the relations themselves. Once all the relationships have been documented, the level of abstraction can be established.

*4. Formulate tests T of the conceptual relation R within CB!*

The conceptual relations were evaluated using the structured phrase template applied from the practical inference method, which asserts a relationship between the investigated terms if one can not be accomplished without the other.

*5. Elaborate the new relation R by tests T respecting CB!*

If that relationship holds, one is an objective, and another is a prerequisite activity to achieve that objective. Inverting the relation should not make logical sense. Activities were compared using the practical inference test and classified into objectives and activities based on this relation.

*6. If the relation R succeeds in tests, declare it a part of CB!*

Once the activities were successfully classified using the method, the resulting activity graph was a formalized representation of the activities' dependencies. These dependencies represent the improved conceptual background that was the goal for applying this method. Subsequently, a list of the activities was produced. Each activity was categorized to likely be an objective or a proper activity. The resulting knowledge of the relations could also be used in sorting the activities topologically.

### 3.3.2 Practical inference method

In this work, the concept of practical inference (Von Wright, 1963), was used as a guide to check whether a given activity should be regarded as such. The application of practical inference was necessary to perform step 4 in the constructive analysis method. Von Wright uses the concept of practical inference in the context of presenting the necessary means to an end in logical arguments.

One way of defining activity is to look at how it fits into a logical argument. Activity, as understood in the context of these NCSS documents, is a means to an end. That is to say; if one wishes to achieve a specific objective, one must take action to accomplish it. The practical inference is a logical argument with its roots in theoretical and practical syllogisms that Aristotle described. To describe the structure of practical inference, we will use one of von Wrights own examples:

*One wants to make the hut habitable.*
*Unless the hut is heated, it will not become habitable.*
*Therefore, the hut must be heated.*
(Von Wright, 1963, p. 60)

The first statement is a premise, the "end" that one wishes to apply the means to accomplish. Without this goal, it is not possible to proceed with the analysis.

The second statement is also a premise, but the first premise depends on its success. The desired end will not be reached unless the action described in the second statement is also completed. Thus, the second part is the "means" to an end described in the first premise.

The third statement expresses practical necessity, and it is extracted from the two premises. An action must be performed to reach an objective. Without action, the objective will not be accomplished. The necessity is strict only when studying the inference from the strict first-person perspective. When the same person wishes to accomplish an objective for which he knows the requisite action, the Aristotelian view always leads to action and leaves no room for choice. However, there is also the possibility that the subject may be unable to perform the necessary actions to reach the objective because he does not know about it.

The primary practical inference method of von Wright, as described, was applied to the activities that had been discovered from the existing research on NCSS documents, and

it proved to be a valuable tool to map out the relationships between the activities. Thus, each discovered link between the activities shows us a relationship between them.

In theory, while this method precludes circular dependencies between two activities, it is possible to have a circular relationship between the activities if three activities depend on each other in a sequence. Loops were not observed in the set of activities investigated in this thesis, but it is still a possibility. Whether or not that will happen should more activities are added to the analysis remains undefined.

# 4. Comparing the existing analyses

This section explores and compares the primary sources that were identified in this study. The main sources were the four different analysis frameworks with a sufficiently large base of the source material. There are several significant differences in how these comparisons group the topics seen in the NCSS documents and their weight to specific topics. Topics in this context are groupings of activities that will be identified later.

Relation to other national strategies is explored in detail in the Luiijf comparison but not mentioned in any significant detail in the ENISA analysis, nor is it mentioned in the topic clustering approach. Since only one primary source does this kind of exploration, it is impossible to perform any comparative analysis.

There was one category, "guiding principles," that only exists explicitly in Luiijf's analysis. Some of the ENISA framework content added under the identified "guiding principles" sub-section could be part of either strategic objectives or program-level objectives but are not comparable to Luiijf's work. The OECD publication does not approach this topic, and Kolini's work is not trying to develop that kind of material so that no meaningful comparisons can be made on it. Much more information on the guiding principles can be found in supporting materials, such as the research into devising cybersecurity strategies from GCSCC.

## 4.1 Overview of the NCSS analyses

The four primary comparative analyses in this thesis overlap in their source material based on how early the respective countries' NCSS documents were published. There is also overlap on what the interesting geographical areas were for the studies' authors. The OECD analysis is focused on the organization's member countries, just as ENISA analysis focuses only on the European countries. Luiijf's and Kolini's work includes all the countries that had published NCSS documents and made them accessible when writing their research papers. Since these publications are from 2011-2017, the research does not cover all the currently available NCSS documents.

While the ENISA analysis is focused entirely on European Union member countries, they also list various documents outside Europe as referenced source material. However, the publication does not mention whether they used them in the background analysis, and the visualized analysis results focus on Europe. Based on that, it is unclear whether the referenced NCSS documents' content was used as a basis for the analysis that leads to the proposed framework include content from those documents or whether they are merely referenced some additional documents for due diligence purposes.

The OECD material is not directly useful for comparison purposes since the analysis focuses on the written responses to their questionnaire rather than evaluating the material in the NCSS documents. However, it produces a valuable categorization model that can be used in association with the other frameworks.

The following Table 2 summarizes the countries that were included in all the analyses and showed the overlapping countries based on analysis and references:

**Table 2**: Countries whose NCSS document has been included in one or more analyses that were evaluated.

| **Country** | **Luiijf** | **ENISA** | **OECD** | **Kolini** |
|---|---|---|---|---|
| Afghanistan | No | No | No | Yes |
| Albania | No | No | No | Yes |
| Australia | Yes | Referenced | Yes | Yes |
| Austria | No | Yes | No | Yes |
| Bangladesh | No | No | No | Yes |
| Belarus | No | No | No | Yes |
| Belgium | No | Yes | No | Yes |
| Canada | Yes | Referenced | Yes | Yes |
| Colombia | No | No | No | Yes |
| Croatia | No | No | No | Yes |
| Cyprus | No | No | No | Yes |
| The Czech Republic | Yes | Yes | No | Yes |
| Denmark | No | No | No | Yes |
| Egypt | No | No | No | Yes |
| Estonia | Yes | Yes | No | Yes |
| Finland | No | Yes | Yes | Yes |
| France | Yes | Yes | Yes | Yes |
| Georgia | No | No | No | Yes |
| Germany | Yes | Yes | Yes | Yes |
| Ghana | No | No | No | Yes |
| Hungary | No | Yes | No | Yes |
| Iceland | No | No | No | Yes |
| India | Yes | Referenced | No | Yes |
| Ireland | No | No | No | Yes |
| Italy | No | Yes | No | No |
| Jamaica | No | No | No | Yes |
| Japan | Yes | Referenced | Yes | Yes |
| Jordan | No | No | No | Yes |
| Kenya | No | No | No | Yes |
| Latvia | No | No | No | Yes |
| Lebanon | No | No | No | Yes |
| Lithuania | Yes | Yes | No | Yes |
| Luxembourg | Yes | Yes | No | Yes |
| Malaysia | No | No | No | Yes |

| | | | | |
|---|---|---|---|---|
| Malta | No | No | No | Yes |
| Montenegro | No | No | No | Yes |
| Morocco | No | No | No | Yes |
| The Netherlands | Yes | Yes | Yes | Yes |
| New Zealand | Yes | Yes | No | Yes |
| Nigeria | No | No | No | Yes |
| Pakistan | No | No | No | Yes |
| Poland | No | Yes | No | Yes |
| Portugal | No | No | No | Yes |
| Qatar | No | No | No | Yes |
| Romania | Yes | Yes | No | No |
| Russia | No | No | No | Yes |
| Saudi Arabia | No | No | No | Yes |
| Scotland | No | No | No | Yes |
| Singapore | No | No | No | Yes |
| Slovakia | No | Yes | No | Yes |
| Spain | Yes | Yes | Yes | Yes |
| South Africa | Yes | Referenced | No | Yes |
| South Korea | No | No | No | Yes |
| Sweden | No | No | No | Yes |
| Switzerland | Referenced | Referenced | No | No |
| Taiwan | No | No | No | Yes |
| Turkey | No | No | No | Yes |
| Trinidad | No | No | No | Yes |
| The United Kingdom | Yes | Yes | Yes | Yes |
| The United States of America | Yes | Referenced | Yes | Yes |
| Uganda | Yes | No | No | No |

Since the publication of the previous analyses, many countries have produced new or updated their existing NCSS documents. A large number of those have not been included in these studies. The included documents cover a bit more than half of all the currently published documents. For some documents, the analysis was done for a previous version of the document that has now been rewritten.

## 4.2 Objectives

Both Luiijf's and ENISA's comparison analyses identify objectives as a significant factor in the NCSS documents. The ENISA analysis splits the objectives into two categories: strategic and program-level objectives distinguished by abstraction. Luiijf identifies only

strategic goals. While acknowledged to be part of the research methodology in previous research, objectives are not included in the research methodology in the computational classification study of Kolini.

There is some additional research into the objectives and activities defined in NCSS documents. For example, Enescu (Enescu, 2020) has studied the NCSS documents published by EU and European countries and identifies the following four high-level objectives under which the other activities can be grouped:

1. National cooperation in European cybersecurity strategies
2. International cooperation
3. Awareness, education, research, and development
4. Critical infrastructure protection and resiliency of the network and information systems

This grouping into objectives is very high-level and does not help understand how the activities are linked to these objectives. Further analysis of this is done later with the activities in chapter 4.6.

## 4.3 Stakeholders

Stakeholder analysis is present in both ENISA and Luiijf's analysis; however, some differences exist in the results' grouping. Luiijf identifies seven stakeholder categories:

- Citizens
- SME
- ISP
- Large organizations
- CI operators
- The state / national security
- Global infrastructure and issues.

In the ENISA analysis, the grouping of the stakeholders is as follows:

- Individual users
- Business / private sector
- Critical infrastructure
- CERT
- Public bodies

Citizens and Individual users are a category that could be the same in both reports, as are the categories of CI operators and Critical infrastructure. However, Luiijf's categorization in the private sector is more granular, splitting the "business / private sector" category present in the ENISA report into three sub-categories of SMEs, ISPs, and large organizations.

Luiijf also mentions the state and national security as a stakeholder, which could be reasonable for this purpose, but it appears that the definition is too vague to be helpful. Therefore, ENISA omits that group and instead mentions a CERT as a stakeholder. A national CERT is undoubtedly a more tangible stakeholder as it is typically a well-defined organization established as part of government legislation. In some cases, they can be organizations with up to 25 years of history and usually operate under one of the relevant ministries or the president's office.

## 4.4 Activities

Action plans that the four analyses use have considerable differences in the definitions. Due to these observed differences, this topic was interesting to pursue a more in-depth analysis.

ENISA discusses activities on a higher level, with the conclusion that *"activities are not discussed in detail in the strategies to be identifiable and allow mapping,"* i.e., there is not enough material for activity analysis in the NCSS documents. Discussion of the activities is also part of the chapter on outcomes and impacts. However, this is not true in the sense that Luiijf did manage to document a long list of activities and objectives. Those activities were mapped with each other.

OECD report has identified action plans in the NCSS documents and reflects those findings against their earlier survey to identify key priority areas from 2004. However, the OECD report does not present the individual activities that they identified. Instead, they group the observed activities into six different categories with descriptions.

Luiijf calls this feature of the NCSS documents *tactical or operational action plans* and goes into detail, identifying and tabulating 36 different activities or goals from the various analyzed NCSS documents. Since both OECD and Luiijf are studying an overlapping subset of the same document collection, the categories can be analyzed by grouping Luiijf's activity findings according to the OECD categories. Also, since Luiijf's work includes findings from a set of 7 NCSS documents not included in the OECD report, it is possible to evaluate how comprehensively the categories have been defined in the OECD report.

The following are the six categories that OECD defines:

1. *Government security - Action plans include a multiplicity of initiatives, from the development of a situational awareness capacity to the rationalization of government network infrastructures, and the generalization of audits in the public sector."*
2. *Protection of critical information infrastructures - "Action plans generally include measures related to the protection of critical information infrastructures."*
3. *Fight against cybercrime - "action plans include many initiatives to develop law enforcement capacities, improve the legal framework and foster international co-operation on the basis of the Budapest Cybercrime Convention."*
4. *Awareness-raising - "Action plans include many initiatives targeting specific populations such as children, SMEs, and decision-makers in government and critical infrastructures."*
5. *Education - "action plans recognize in particular the need for a stronger cybersecurity workforce. The development of cybersecurity skills is identified as a key priority by several countries."*
6. *Response - "Strategies recognize the role played by Cybersecurity Incident Response Teams (CSIRTs), and create a national CSIRT or strengthen it where it already exists."*
7. *Other categories - Actions that did not have a clear fit into the OECD categories*

(Bernat et al., 2012)

The OECD categories are based on evaluation and questionnaires collected from NCSS related authorities from various countries. As they are one of the first publications on the topic, they form a baseline to which the work of others can be compared. While not an evaluation framework, the structure presented in the GCSCC guide can be compared to the OECD categories. GCSCC guide proposes the following dimensions for a cybersecurity strategy. In the document, each one is then decomposed into sub-items:

1. *Devising cybersecurity policy and strategy*
    1. *National cybersecurity strategy – development, organization, content*
    2. *Incident response – identification of incidents, organization, coordination, mode of operation*
    3. *Critical infrastructure protection – identification, organization, risk management, and response*
    4. *Crisis management*
    5. *Cyber defense consideration – strategy, organization, coordination*
    6. *Communications redundancy*
2. *Cyberculture and society*
    1. *Cybersecurity mindset – government, private sector, users*
    2. *Trust and confidence on the Internet – user trust and confidence on the Internet, user trust in e-government services, user trust in e-commerce services*
    3. *User understanding of personal information protection online*
    4. *Reporting mechanisms*
    5. *Media and social media*
3. *Cybersecurity Education, Training and Skills*
    1. *Awareness Raising – Awareness Programs for public and executives*
    2. *Framework for Education – Provisioning and administration*
    3. *Framework for Professional Training – Provisioning and uptake*
4. *Legal and Regulatory Frameworks*
    1. *Legal Frameworks – For all aspects of society*
    2. *Criminal Justice System – Law enforcement, prosecution, and courts*
    3. *Formal and Informal Cooperation Frameworks to Combat Cybercrime*
5. *Standards, organizations, and technologies*
    1. *Adherence to Standards – ICT Security standards, procurement standards, and standards in software development*
    2. *Internet Infrastructure Resiliency*
    3. *Software Quality*
    4. *Technical Security Controls*
    5. *Cryptographic Controls*
    6. *Cybersecurity Marketplace – Cybersecurity technologies and cyber insurance*
    7. *Responsible Disclosure*

(Global Cyber Security Capacity Centre, 2016.)

This list is an interesting comparison with the categories discovered in the OECD document, as seen in Table 3. Government security, protection of the critical information infrastructures, and response categories map well into the evaluation guide's first dimension while fighting against cybercrime maps directly to dimension four. Both awareness-raising and education categories map into the identical third dimension. That leaves both GCSCC dimensions two (Cyberculture and society) and five (Standards, Organizations, and Technologies) outside the categories presented in the OECD work.

There may be many reasons for this mismatch. For example, there may be a lack of source material available in 2012, compared to the available material in 2016. For additional insight, it was considered whether the topics from the cluster analysis by Kolini (Kolini and Janczewski, 2017) are analogous to the OECD report categories.

**Table 3**: Cybersecurity strategy topic categories from OECD study vs. GCSCC defined dimensions for cybersecurity strategies

| | OECD category | GCSCC dimension |
|---|---|---|
| 1. | Government security | 1. Devising cybersecurity policy and strategy |
| 2. | Protection of critical information infrastructures | 1. Devising cybersecurity policy and strategy |
| 3. | Fight against cybercrime | 4. Legal and regulatory frameworks |
| 4. | Awareness-raising | 3. Cybersecurity Education, Training and Skills |
| 5. | Education | 3. Cybersecurity Education, Training and Skills |
| 6. | Response | 1. Devising cybersecurity policy and strategy |

The source material of Kolini's study highly overlaps with the OECD analysis; it includes NCSS documents from all OECD countries included in the OECD NCSS analysis. In their analysis, a Latent Dirichlet Allocation (LDA) machine learning algorithm was applied to perform the clustering based on the NCSS source documents. The clustering algorithm produces a set of words seen to appear in the same context in the documents. The approach is also called topic modeling, effectively extracting a topic from the surrounding material, in this case, the NCSS document. The algorithm is unsupervised, and it does not imply any understanding of the contents of the documents, and the results are a set of words that define a topic.

The topics identified in the analysis of Kolini are listed as follows. The authors labeled each topic based on their evaluation of what would be the best match. The list below omits the cluster of words that they were composed of:

1. *Defending citizens and public IT systems*
2. *Organization/Sector for cybersecurity*
3. *Cyberspace resiliency against attacks for critical sectors and infrastructure*
4. *Develop policy and standard for technology and infrastructure*
5. *Legislation and laws for cybercrime*
6. *Public-Private and International cooperation*
7. *Cybersecurity measure for cyber capabilities*
8. *Training and awareness for the public, private sector, and online businesses*
9. *Risk management procedures*
10. *Critical infrastructure protection*

(Kolini & Janczewski, 2017.)

There are similarities to the topics identified in the OECD analysis and Kolini's proposed categories. Most of the categories can be mapped into the OECD proposed categories, although the wordings are not exact. Some of them would need to be mapped to the "other" category, which is a catch-all for everything else.

Finally, beyond the evaluation frameworks, there is also more narrow research into NCSS documents that can be contrasted with the categories provided by OECD and Kolini. For

example, in his analysis of 8 NCSS documents, Lehto identified a set of six priorities found in almost every cybersecurity strategy. These are the high-level priorities that are close in meaning with the categories as proposed by OECD, and others:

- *Roles and responsibilities of cybersecurity*
- *Cybersecurity Center / situational awareness*
- *Legislation and supervising the lawfulness of government actions*
- *Cybersecurity training and research*
- *Secure IT products and services*
- *National and International cooperation*

(Lehto, 2013, s. 189)

Topics provided by Lehto are related but do not entirely overlap with the other studies' topics. The lack of overlap shows how difficult it is to arrive at a consensus opinion on what topics are present in the NCSS documents. Each of the researchers brings their perspective into defining the topics, and their results are pretty different.

Another perspective to consider is whether NCSS documents should include definitions or descriptions of activities at all. For example, one can argue that a strategy document should be restricted solely to present the objectives rather than describe the activities to achieve them. Activities would then be described in a separate cyber strategy implementation document. The split strategy and implementation plan approach is taken by Finland in their published NCSS documents from the year 2013 (Government of Finland, 2013) and 2019 (Government of Finland, 2019), and the accompanying implementation plan (Government of Finland, 2016).

Other countries may also have taken this approach, which could mean that analysis of some of the NCSS documents – if taken as a stand-alone document – may not capture the intended activities to accompany the strategy. However, some NCSS documents explicitly mention activities, such as the Lithuanian NCSS (Government of Lithuania, 2011), and Ireland (Government of Ireland, 2014.) The existence of both kinds of documents makes the NCSS documents more complex to analyze.

With the proposed categorization scheme extracted from several different sources, it became possible to map the actions and action lines observed by Luiijf and see how they would distribute into the categories proposed by the OECD and Kolini. The mapping was performed for the list of activities discovered by Luiijf. The complete mapping is presented in Table 4 in the following analysis chapter.

# 5. Analysis of the activities

In the previous chapter – while investigating how the different analyses handled the topic of activities – it became evident that each study's authors must have had different definitions of what constitutes an activity. Following their respective definitions, they either found many activities in the source material or not many at all.

While they did not share those definitions as part of the research publication, they assumed that they did not apply the same definition based on their analyses. No one has proposed a definition in prior research for these activities as far as could be discovered in the literature search for this analysis.

While it is not possible to assert the absolute truth, since the mapping is by necessity a subjective exercise that depends on the experience and expertise, the most likely result should be somewhere between these two positions. This disconnect between these analyses merits further investigation, as it is possible to propose methods to define these activities. Those methods could help write future NCSS documents or when further analyzing the existing document base.

In the research comparing the frameworks, it was notable how the objectives and activities were defined at different levels in the ITU's definition of cybersecurity strategy (International Telecommunications Union, 2018). Therefore, in the analysis of the results in chapter four, that lack of distinction was studied more closely.

## 5.1 Classifying the activities

The following table is one of the key results from the research into the activities discovered in previous analyses. Table 4 enumerates all the "action and action lines" items from Luiijf's work and combines them with the categories found from the OECD and Kolini's research. It also contains further analysis data derived from the results of the relationship mapping.

There are quite a few columns in Table 4, starting from the name of the activity from Luiijf's research and a unique id number. The table shows the mapping of activities into the respective categories identified in the OECD analysis and described in chapter 4.6, followed by mapping the activities into the respective topics identified by Kolini in their clustering analysis.

The table also presents "proximity groups," the three high-level categories that the activities appear to fall into when organized topologically on the graph: activity (A), support (S), and policy (P), indicated with letters.

Finally, the number of relationships of the activity in the relationship graph is listed in the second to last column of Table 4. These are the number of activities that form connections to this activity, as shown later in Figure 1 in chapter 5.7. The last column shows the calculated inbound/outbound connectivity percentage. The connection density is represented by colors later in Figure 1 in chapter 5.7. These helped to create the level of abstraction diagram.

**Table 4**: Mapping of actions identified by Luiijf into the categories identified in OECD and Kolini's research.

| Action and action lines | # | OECD Group | Kolini Group | Proximity groups | Relation count (Out / In) | Out / In percent |
|---|---|---|---|---|---|---|
| Active / dynamic security measures | 1 | 1,2 | 1,3 | A | 1/1 | 50 |
| Awareness and training / information security campaign | 2 | 4,5 | 8 | P, A | 7/2 | 28.5 |
| Adaptable policy to new ICT risk | 3 | 7 | 4 | P, S | 3/3 | 50 |
| Continuity and contingency plans | 4 | 1,2,6 | 1,3,9,10 | P, A, S | 3/4 | 75 |
| Critical infrastructure protection | 5 | 2 | 10 | A, S | 3/9 | 33 |
| Cryptographic protection | 6 | 7 | 3 | A | 6/0 | 100 |
| Cyber arms control | 7 | 3 | 4,5 | P | 0/3 | 0 |
| Defense cyber operations / intervention, training and exercises | 8 | 4,5,6 | 3,8,9 | A | 0/4 | 0 |
| Develop and share good practices | 9 | 4,5 | 4,7,8 | A | 3/3 | 50 |
| Economic growth | 10 | 7 | N/A | S | 0/4 | 0 |
| Education and training | 11 | 5 | 8 | P | 3/0 | 100 |
| Exercises | 12 | 4,5 | 8 | A | 5/1 | 17 |
| Explicit holistic view | 13 | 7 | N/A | P | 3/0 | 0 |
| Exploitation to combat threats | 14 | 1,3 | N/A | A | 1/0 | 0 |
| Improved security of ICT products | 15 | 1,2,3 | 1,3 | P | 4/5 | 56 |
| Information sharing / exchange | 16 | 1,2,3,4,6 | N/A | A, S | 4/3 | 43 |
| Intelligence gathering on threat actors | 17 | 1,2,3,6 | N/A | A | 3/0 | 0 |
| International collaboration | 18 | 6 | 6 | A | 3/1 | 25 |
| Legislation / legal framework | 19 | 1,3 | 5 | P | 3/0 | 0 |
| Mandating security standards | 20 | 4,6 | 4 | P | 4/2 | 33 |
| National detection capability | 21 | 2,6 | 10 | A | 1/4 | 80 |
| National response capability / ICT crisis management | 22 | 6 | 2 | A | 3/4 | 57 |
| Privacy protection | 23 | 3,4 | 4,5 | P | 1/2 | 67 |
| Promote cyber-crime convention | 24 | 4 | 5 | P | 2/2 | 50 |
| Protection of non-critical infra | 25 | 1,6 | 1,2 | A | 0/3 | 100 |
| Public-private partnership | 26 | 7 | 6 | S | 2/3 | 60 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Reducing adversary's motivation and capabilities | 27 | 3 | N/A | P | 0/6 | 100 |
| Research and development | 28 | 5 | N/A | S | 6/2 | 25 |
| Resilience against disturbances / threat and vulnerability reduction | 29 | 3,6 | 3 | A | 1/6 | 86 |
| Secure protocols and software | 30 | 2,3,6 | 1,3 | P, S | 2/3 | 60 |
| Secure sourcing of products | 31 | 2 | 4 | P | 1/1 | 50 |
| Self-protection of the government | 32 | 1 | 2 | A, S | 0/3 | 100 |
| Strategic cybersecurity council | 33 | 1 | N/A | P, A, S | 7/0 | 0 |
| Threat and vulnerability analysis | 34 | 4,6 | 9 | S | 3/1 | 25 |
| Tracing criminals and prosecution | 35 | 3 | 5 | P | 0/3 | 100 |
| Actions defined in a SMART way? | 36 | 7 | N/A | P, S | 2/1 | 33 |

## 5.2 Mapping of Luiijf's activities to OECD and Kolini's categories

Table 4 presented all the mappings between Luiijf's discovered activities to the categories proposed by OECD and Kolini. This mapping is subjective, as the actions presented by Luiijf do not have comprehensive descriptions. The activities also do not contain any links to the original material to validate the author's observations. Thus, the only feasible method to trace back the claims would be to comb through all the referenced documents and identify the specific passages in the particular document that match the definition. The tracing was tested for some of the actions to see whether it is feasible, and it was, but reproducing the whole study is far beyond the scope of this work.

Luiijf presents a list of strategic objectives that different countries have laid out in their NCSS documents. In this list of strategic objectives, it could be observed that there are quite a few of the same items that are later included in the list of activities and action lines. It is unclear whether these strategic objectives have been kept separate for some purpose during the analysis where activities were identified and listed from the source material. Another possibility is that, in the author's opinion, they are otherwise independent of each other. It also requires some analysis and verification to infer whether items in the listed activities are taken from the listed strategic objectives.

After mapping the actions into the proposed categories, the first observation was that many activities fit comfortably under several proposed categories. There are a few possible explanations for why the ambiguity exists:

1. It is possible that the categories logically cannot be defined in a way that is precise enough, which by necessity means that there is ambiguity in how to sort the activities into categories
2. The activity may be something that naturally falls into multiple distinctive categories because it encompasses multiple topics in itself, and it does not make

sense to merge those categories into a higher abstraction level that would subsume the specific definitions
3. The OECD purposefully defines the categories in their report to make it practically impossible to assign an activity to a single category. That could be due to the intentionally ambiguous definition of the category, which in turn leads one to place the activities under several categories
4. The activity in question may not be an actual activity but instead describes an objective that is part of the strategy, making it difficult to place into a proper category

For three of the proposed explanations for the ambiguity, some solutions can be applied to resolve the activities' fuzzy match against the presented categories.

One could attempt to devise better categories to address the first explanation. Since there is now a larger pool of usable information in the form of NCSS documents to base the categories on, this could lead to further insights in creating the categories. Many more countries have published NCSS documents since the publication of the evaluation frameworks, which are now available for analysis. The scope of available material from the ten used initially in the OECD study has expanded to 104 when writing this thesis. However, the authors likely had a reason for limiting the number of categories to six in their study. While working with the source documents, the authors may have decided to merge many categories to get the total number down to six, which they considered a good number. Adding more categories can make the categories harder to apply in practice. Additional source material may also produce new categories that would need to be added so that one can group the activities properly.

The second cause is something one cannot directly address by altering the categories; one needs to specify the more specific activities that are easier to classify into distinct categories. Since the listed activities have been extracted from the existing NCSS documents, it is not feasible to improve the situation in this NCSS document analysis scope. To improve the situation, one would need to develop an activity ontology that directly maps into the categories listed above or into another set of categories. Then the developers of the future NCSS documents could be encouraged to adhere to that ontology.

It is unlikely that even a majority of the NCSS document writers would follow such a plan. Additionally, it is not even known whether the currently proposed categories are suitable to serve that purpose. It will require research to determine whether using the approach of guided activity design would be a beneficial activity since the NCSS documents are not written with the goal of being friendly to academic analysis. The primary purpose of NCSS documents is to communicate the strategy and the activities that the stakeholders should be engaged in using as straightforward terms as possible. That may be a more potent driver than the ability to follow predefined norms.

As for the third case, the situation could be improved by inspecting each proposed activity and attempting to determine whether it is a proper activity or not. Again, there are some practical benefits to this, as it would enable us to recommend better activity definition guidelines to the authors of the future NCSS documents. As that is feasible to accomplish, it was performed in this thesis and is described in the following sections.

## 5.3 Definition of an Activity

We want to separate the claimed activities into two categories: actual activities and objectives merely presented as activities. Therefore, it is necessary to apply a precise

definition of activity to distinguish between them and perform the sorting objectively. The definition and sorting were facilitated by the constructive analysis method, combined with the practical inference test.

It is necessary to use a formal way of inspecting the activities when attempting to separate the activities from the objectives. Therefore, assessing the activities identified in the four primary sources needed to be done by explicitly defining what an activity is and then observing whether the results of the comparisons match the definition. In this way, it is possible to overcome the lack of data on the previous research methods. Furthermore, this formal activity classification may be novel, as none of the referenced analyses disclose the particular research method used to arrive at their classification.

The practical inference method can be used to distinguish between them by following the generic template as proposed by von Wright (Von Wright, 1963):

"*One wants to attain x.*
*Unless y is done, x will not be attained.*
*Therefore, y must be done."*

Because the template proposed by Von Wright is very generic, the practical inference is an analytical tool that can be consistently applied for each of the proposed activities. The only requirement is that the activities' evaluator has sufficient domain expertise to understand if the result makes logical sense. Determination of whether they are proper activities was done by applying practical inference clauses to the activities as proposed by Luiijf.

The template requires that we see them work when placed on the second statement if they are considered activities. If the statement functions as intended with the proposed activity in the second clause, it should be possible to describe an objective that is reached due to that activity. On the other hand, objectives fit naturally into the first clause of the template and function as goals for proper activities in the second clause.

This template can substitute any of the listed activities for y and x and see a logical fit. Since the activities appear to be a mix of objectives and activities, it should be possible to use some of them in the first clause and some in the second clause. For example, objective "cyber awareness" and the activity, "Education and training" does appear to fit the proposed structure:

*We need to improve the cyber awareness of the country,*
*However, unless we engage in education and training, cyber awareness will not increase.*
*Therefore, we must invest in education and training.*

This leads us to infer that the following relationship exists:
**"education and training" → "cyber awareness"**

Whereas "Critical Infrastructure Protection" would fit better when substituted into the first premise of the template:

*We need to protect critical infrastructure,*
*However, unless we develop continuity and contingency plans, the critical infrastructure will not be sufficiently protected.*
*Therefore, we must engage in the development of continuity and contingency plans.*

Based on this observation, “Critical Infrastructure Protection” can be classified as an objective, and correspondingly “Education and Training” and “Continuity and Contingency Plans” as activities.

**“continuity and contingency plans” → “protecting critical infrastructure”**

While this is not a perfect way to separate the activities from the objectives, it does provide a straightforward method that can be consistently applied to each of the proposed activities.

However, to validate this approach, it should be shown that the results would be consistent and that the same logical structure still works if it is reversed. Therefore, we substitute the supposed objective and activity into second and first clauses instead. Then, using the example from above, we observe that the opposite statement does not make logical sense:

*We need continuity and contingency plans,*
*However, unless we are protecting critical infrastructure, there will not be proper continuity and contingency plans.*
*Therefore, we must protect critical infrastructure.*

Protecting critical infrastructure is not necessary for continuity and contingency plans; the plans may well exist due to a thought experiment without ever having been put into use. Protecting critical infrastructure can be considered an activity – if a very high level one – but it does not work as a premise to developing continuity and contingency plans.

**“protecting critical infrastructure” ↛ “continuity and contingency plans”**

Setting up a few more examples provides additional insights into the issue. For example, this statement can be changed to make logical sense by exchanging the second clause with a more reasonable activity from our list, such as “Threat and vulnerability analysis”:

*We need continuity and contingency plans,*
*However, unless there are threat and vulnerability analyses, there will not be effective continuity and contingency plans.*
*Therefore, we must engage in threat and vulnerability analysis.*

**“threat and vulnerability analyses” → “continuity and contingency plans”**

This change enables the statement to make logical sense and establishes how this approach can sort different activities based on two factors. First, if the activity is at a higher level of abstraction than the other, it becomes apparent during the comparison. Second, suppose activity is a requirement for another activity. In that case, the relation can be established with the comparison, and the activity that requires the other activity can be considered more likely to be an objective.

Table 5 presents the classification results for all the activities extracted from Luiijf’s NCSS evaluation based on the methodology described above. Again, classification is marked as either activity or objective.

**Table 5:** Identifying objectives in Luiijf's "Actions and Action lines."

| | **Action and action lines** | **Classification** |
|---|---|---|
| 1 | Active / dynamic security measures | Activity |
| 2 | Awareness and training/information security campaign | Activity |
| 3 | Adaptable policy to new ICT risk | Objective |
| 4 | Continuity and contingency plans | Activity |
| 5 | Critical infrastructure protection | Objective |
| 6 | Cryptographic protection | Activity |
| 7 | Cyber arms control | Objective |
| 8 | Defense cyber operations/intervention, training, and exercises | Activity |
| 9 | Develop and share good practices | Activity |
| 10 | Economic growth | Objective |
| 11 | Education and training | Activity |
| 12 | Exercises | Activity |
| 13 | Explicit holistic view | Objective |
| 14 | Exploitation to combat threats | Objective |
| 15 | Improved security of ICT products | Objective |
| 16 | Information sharing/exchange | Activity |
| 17 | Intelligence gathering on threat actors | Activity |
| 18 | International collaboration | Activity |
| 19 | Legislation / legal framework | Objective |
| 20 | Mandating security standards | Objective |
| 21 | National detection capability | Objective |
| 22 | National response capability / ICT crisis management | Objective |
| 23 | Privacy protection | Objective |
| 24 | Promote cyber-crime convention | Activity |
| 25 | Protection of non-critical infra | Objective |
| 26 | Public-private partnership | Objective |
| 27 | Reducing adversary's motivation and capabilities | Objective |
| 28 | Research and development | Activity |
| 29 | Resilience against disturbances/threat and vulnerability reduction | Objective |
| 30 | Secure protocols and software | Objective |
| 31 | Secure sourcing of products | Objective |
| 32 | Self-protection of the government | Activity |
| 33 | Strategic cybersecurity council | Objective |
| 34 | Threat and vulnerability analysis | Activity |
| 35 | Tracing criminals and prosecution | Activity |
| 36 | Actions defined in a SMART way? | Objective |

This work to apply the criteria – even while applying a formal method – is intricate and shows that the objectives and activities are not straightforward to categorize due to the ambiguity in the level of abstraction. For example, whether "Exploitation to combat threats" is an objective or activity is highly dependable on the context. For example, for an organization that can engage in exploits, this would be an activity. However, in the

context of the NCSS document, it is much closer to an objective since the intention is to develop such capability.

The above list serves as a helpful starting point for analyzing the activities and objectives with these caveats. Furthermore, it enables us to arrange them hierarchically and discover new insights from how they are organized.

## 5.4 Validation of the practical inference method

After classifying the objectives and activities from Luiijf's work with the practical inference method, it becomes possible to compare the results against the actual objectives and "tasks" defined in the Lithuanian cybersecurity strategy. Lithuania was chosen because very few NCSS documents summarize their objectives and activities in an easily accessible table. Table 6 presents the Lithuanian NCSS author's opinion on the objectives and activities intended to achieve those objectives.

This comparison will serve two different functions. First, it allows us to compare the objectives and activities listed in the existing analyses and see if they can be connected with a reasonably matching counterpart in Luiijf's list. Secondly, it is possible to check whether the objective-analysis classification performed for the list matches the classification used by the authors of the Lithuanian document. If there is a good match, this verification gives some assurance that the applied method is sound.

Additionally, the Lithuanian NCSS document was included in the analyses of Luiijf, ENISA, and Kolini but not in the OECD analysis. Having been part of the analysis of the referenced frameworks makes it a good review candidate. The following Table 6 is an extracted list from the Lithuanian Cyber Security Strategy (Government of Lithuania, 2011)

After mapping the Lithuanian objectives and tasks, it is possible to make observations on the validity. At least one related activity in Luiijf´s list for each item in the Lithuanian strategy indicates that the list has a fair amount of coverage over common objectives and activities that appear in NCSS documents. However, it was difficult to say how accurate that association is due to the activities being defined in ambiguous ways in several cases.

All objectives defined in the Lithuanian NCSS were also mapped to Luiijf’s activities classified as objectives using the practical inference method. However, only three of the ten tasks from the Lithuanian NCSS were classified as activities with the practical inference method, while seven were classified as objectives. This result can indicate several things. First, it can mean that the Lithuanian NCSS proposes tasks that are closer to objectives from the perspective of the action and action lines as defined by Luiijf. Second, it can indicate that the practical inference method applied for the classification is not accurate enough in its current form to reveal when something classified as an objective is a task.

There were 19 associations in total, of which 4, or 24% percent, were low confidence because of the phrasing's ambiguity (marked with a question mark in the table). On the other hand, these ten items classified as tasks retrieved from the Lithuanian document matched clearly into nine of Luiijf’s activities, with two additional uncertain matches against Luiijf’s list.

**Table 6**: The thirteen objectives and tasks in Lithuanian NCSS mapped into the classification created using the practical inference method

| ***Number*** | ***Item*** | **Classification in Lithuanian NCSS** | **Connected Luiijf's action line** | **Classification by practical inference** |
|---|---|---|---|---|
| 1 | To ensure the security of national information resources | objective | 5, 25, 29, 32 | O, O, O, A |
| 2 | to improve the coordination and monitoring of electronic information security (cybersecurity) | task | 21(?) | O |
| 3 | to improve the regulatory framework of electronic information security (cybersecurity) | task | 19 | O |
| 4 | to expand and improve a secure national information infrastructure | task | 30, 32 (?) | O, A |
| 5 | to encourage the implementation of electronic information security (cybersecurity) project | task | 22(?), 25(?) | O, O |
| 6 | to develop international cooperation in the area of electronic information security (cybersecurity) | task | 18 | A |
| 7 | To ensure efficient functioning of critical information infrastructure | objective | 5 | O |
| 8 | to ensure the security of critical information infrastructure | task | 5 | O |
| 9 | To ensure the cybersecurity of the Lithuanian residents and persons staying in Lithuania | objective | 25 | O |
| 10 | to enhance the culture of protection of electronic information security (cybersecurity) | task | 2 | A |
| 11 | to strengthen Lithuania's cybersecurity | task | 22 | O |
| 12 | to ensure the protection of Lithuania's computer network (virtual cyber perimeter) from external cyber attacks | task | 29 | O |
| 13 | to reinforce the security of services delivered in cyberspace | task | 30, 31 | O |

The discrepancy could mean two things; either the Lithuanian document is redundant and repeats similar ideas in a more verbose format. Alternatively, Luiijf's action lines' expressiveness may not be enough to cover the individual activities and objectives from the Lithuanian strategy. For example, it would be expected that when extracting activities from an NCSS source, a document with 10 of those explicitly stated would result in 10 unique items in Luiijf's list. Unfortunately, that was not the case; the match was not perfect.

The discrepancy could mean that the authors had already written down the actions that Luiijf published when they arrived at the Lithuanian NCSS. Therefore, the existing labels did not match the ones presented in the NCSS document. We can speculate that perhaps the existing labels in the generalized list present in Luiijf's work could not be changed enough to accommodate the list present in the Lithuanian NCSS.

## 5.5 Results of the inference classification

The validation effort leads to an observation of the nature of objectives and activities. Instead of the objectives becoming ordered, these concepts form links where an activity can be an objective for a "lower-level" activity. The "level" in this context is about the level of abstraction of the concept, where higher-level concepts encompass other activities and form a hierarchy or a network.

The objectives and activities often share a relationship where one is a requisite for another. When comparing the activities using the practical inference method, it notable that it is easier to notice when an objective-activity pair is mismatched – when there is no perceivable causal relationship. The reason for that is because we can also evaluate the already existing understanding of the relationships to do it. Identifying pairs where the causal relationships should exist – as was shown in the conflicting example – is a more complicated problem. Adding new objectivities and activities to the set to be classified also leads to potential relations' exponential growth. Evaluating the potential new relations requires reevaluating the entire activity base.

Thus, it seems that the problem is not about figuring a way of sorting activities into either objectives or activities. Instead, the problem arises from their property: they are both objectives and activities simultaneously, just at different levels of abstraction. An activity can usually be broken down into sub-activities. In that scenario, we can see how the higher-level activity can become an objective for those lower-level activities. The interesting unknown properties of the activities are then about the level of abstraction and the valid causal relationships between them.

Suppose we assume from now on that there are many different levels of abstraction present in the activities. In that case, that leads to the possibility of some of the activities subsuming other activities within their scope. Hence, it is a property of the activities that they may contain other activities. By identifying the causal relationships between the activities, we can also attempt to analyze and group them by that property.

## 5.6 Mapping the Activity Relationships

While analyzing the definition of activity and studying how to relate them to each other, it was noted that the relations form a network of dependency relationships. The next step is then to perform this kind of mapping. The work to establish the causalities is novel. Unfortunately, that work was not provided in any analyses referenced as the source material or discovered in the literature.

The mapping of the relationships to correct activity pairs requires some domain expertise. As part of the research, this mapping was performed for each activity by considering the causal directions of these various activities' relationships. The best effort attempt was made to find all the causal connections between the activities. However, the result should not be considered a complete analysis. One must keep in mind that it continues to be a subjective exercise because of the activities' higher-level nature. The subjective nature remains even when using constructive analysis and practical inference to elucidate those

connections. Another person or group may arrive at a somewhat different mapping based on their domain expertise.

Figure 1 is a diagram containing all the activities and the links identified from Luiijf's work. One can discover exciting properties that arise from links between these activities. However, the work to manually map the activities' interconnectivity as a diagram based on Luiijf's activities shown on the figure approaches the upper limit of what is feasible without switching to automated graph analysis and visualization tools.

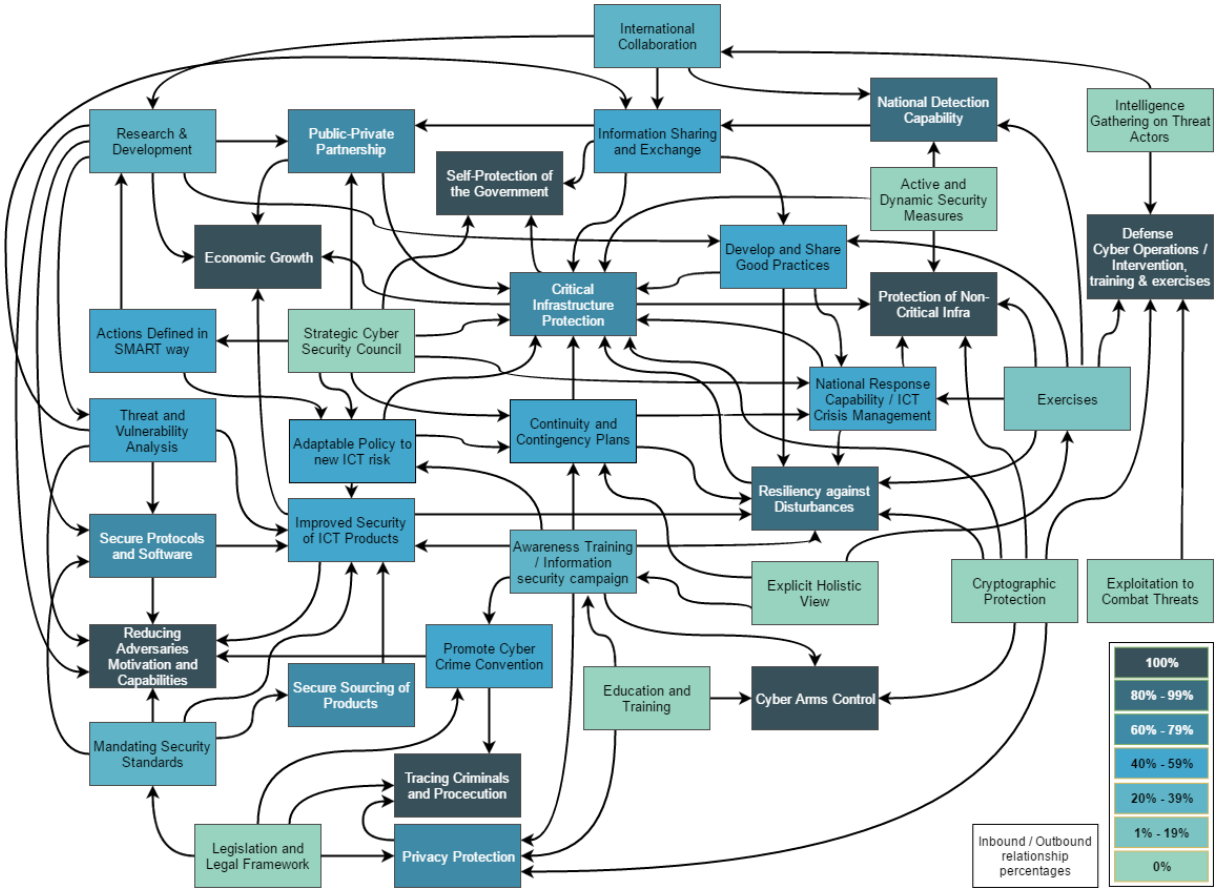


**Figure 1**: Relationships between the activities collected by Luiijf

The activities in Figure 1 are color-coded by the ratio of outbound to inbound relationships in the graph. The darkest colored ones are the activities that have only inbound relationships and do not serve as prerequisites for any of the listed activities.

These activities appear to be very high-level objectives as they have many lower-level requisites. On reflection, these activities could be considered to contain many of the other activities. The capability to contain other activities provides evidence that we should consider these more objective-like tasks that can only be accomplished with extensive coordination of people working on the requisite activities.

The light green coded activities have only outbound relationships at the other end of the connectivity ratio scale. Outbound connectivity means that they have no apparent dependency on any of the other activities. The implication is that these are more foundational activities that enable others. These activities are prerequisites to all the other activities either directly or through secondary and tertiary connections via other activities.

Pruning the secondary and tertiary relations from the diagram in a graph representation is one factor to consider. One example of this duplicated connectivity is the activity named "*Threat and Vulnerability analysis,"* which is directly connected to "*Reducing Adversary's Motivation and Capabilities."* However, it is also connected to that activity via secondary connections through *"Improved Security of ICT Products"* and *"Secure protocols and Software."*

In this case, it makes sense to show all the identified secondary connections in the relationship diagram rather than only show the immediate connections because the visible direct relation provides relevant additional context. The justification for the existence of the direct link is that the "Threat and vulnerability analysis" can meaningfully contribute to the higher-level activity in many ways:

- Threat and Vulnerability analysis contribute to the improved security of ICT products by exposing known vulnerabilities and exposing weaknesses in implementations. In addition, having more secure software is a deterrent to cybercrime because criminal activity is bound to the same economic motivators.
- Threat and Vulnerability analysis contribute to the development of secure protocols and software by motivating them to address the weaknesses already in the development phase and by enabling developers to write more secure software by introducing tools that address known threats at the development time. For example, see OWASP top 10 (The Open Web Application Security Project, 2021)
- Research into threats and vulnerabilities reduces the adversary's capabilities by exposing known attack patterns and methods, patching the vulnerabilities, and providing the network administrator concrete steps to respond to the threats. It also prevents exploitation in secrecy and makes hacking and long-term exploitation more complicated because detection capabilities are usually only available for known vulnerabilities.

If we removed the secondary connections, the implication would be that "Threat and Vulnerability Analysis" only contributes to either "Secure protocols and software" or "Improved Security of ICT Products," but not directly to "*Reducing Adversary's Motivation and Capabilities."* However, that is not true because the activity described above that has a direct impact is not included in the descriptions of these two related activities.

The secondary links are artifacts that arise when moving a common activity that touches many other activities into its separate entity. As the count of activities that are being considered increases, so would the presence of second and third-degree relations.

## 5.7 Activity Graph

After adding the causalities between the various activities, the resulting network has become a directed graph in practice. We can see that there is no single root activity or objective that could turn this graph into a tree-type hierarchy. There are several reasons for the existence of multiple top-level activities.

- It is common for NCSS documents to define multiple objectives for the country to accomplish, and the diagram reflects that. However, after adding the relationships, we can observe that seven objectives only depend on other activities and do not share relationships.
- The listed activities come from multiple NCSS documents that – while they do have very similar intentions – do not describe the same set goals as each country

approaches the NCSS document from their unique perspective. As a result, there is considerable overlap, but they diverge as realistic goals must be defined, considering their existing capabilities.

In this specific version of the graph presented in Figure 2, the directed graph is also acyclic. However, the lack of cyclical connections should not be considered a property of a graph of activity relationships. There are no practical limitations as to why cyclical causal relationships within the various activities could not exist. This observation is especially relevant for the higher-level activities and objectives. It is easy to think of cyclic relationships, so the acyclic property of this graph is accidental. As a practical counter-example, one could easily and without controversy propose a cyclical relationship between economic growth and research and development. However, that relationship is not essential to document in a cybersecurity strategy document.

The cyclical relationships are omitted in the proposed diagram because they do not contribute to our understanding of the functional relationships between the activities. It makes it easier to see the differences in the abstraction level when the relationships have only one direction. The lack of cyclical relationships also made it straightforward to apply topological sorting algorithms to the graph and sort them into a hierarchical list.

Creating the diagram in Figure 2 provided a helpful side product; the activities – in this case, when manually laid out in a way that attempts to minimize overlapping connections to make it readable – cluster into partially overlapping sets of categories or domains. Reducing the number of overlapping connections by moving the activities to different locations generally forces them to be closer to those activities that they share most relationships. A more accurate representation of these grouped activities could be found by applying a heuristic computational algorithm to this process and having it computed to find a minimum overlapping solution.

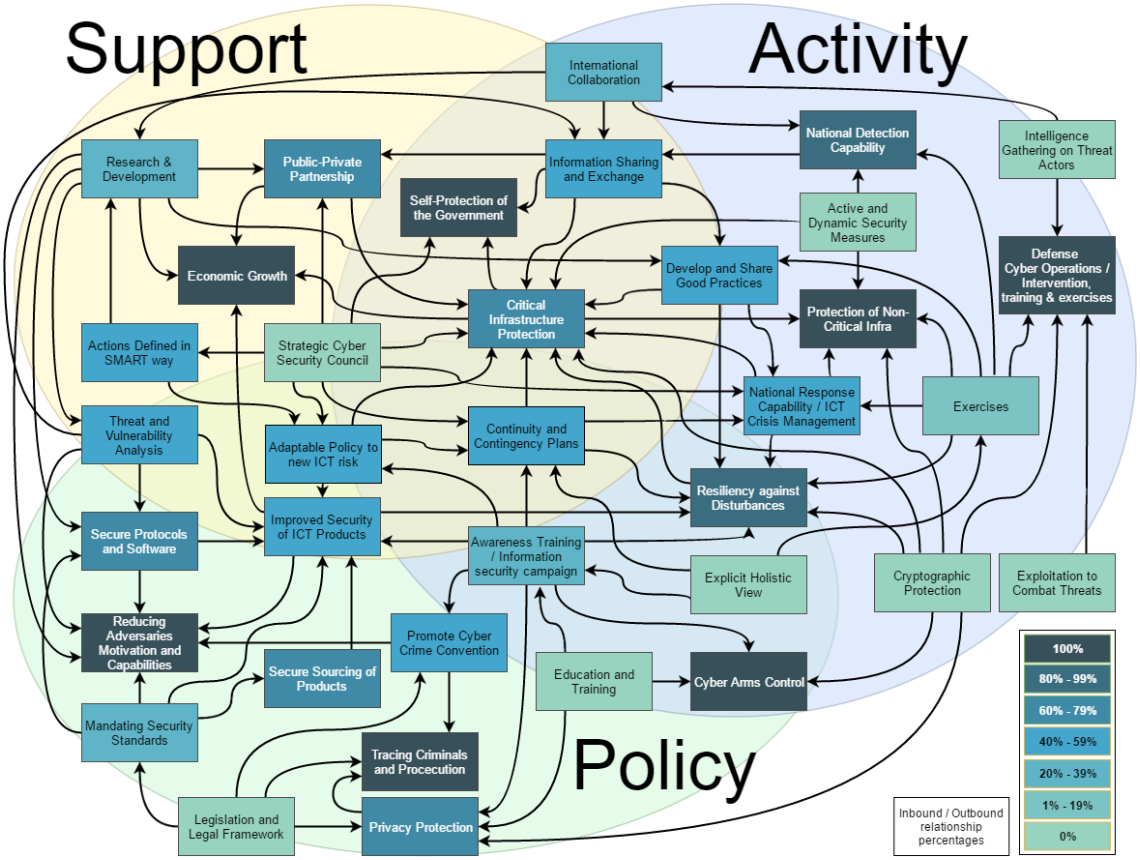


**Figure 2**: Activities naturally cluster into three high-level categories

In Figure 2, the categories have been drawn underneath the activities and labeled. Thus, three high-level categories can be identified, and the categories are highlighted in three different colors:

1. Light green – *Policies* and plans for *defining* the national cybersecurity objectives
2. Light blue – *Activities* that *implement* the policies in practice for improving the national cybersecurity
3. Light yellow – *Supporting* activities and objectives for the effort of improving national cybersecurity

This proximity-based alternative categorization into three groups is a less precise way to describe the activities than the six-category version provided by OECD. However, it developed organically and emerged from the data, and was worth documenting. Furthermore, investigating this approach by applying previously known clustering algorithms to the data by labeling the activities with keywords could help see how the activities can be split into other sets of distinct categories.

## 5.8 Grouping activities by their proposed causal relationships

In defining the activities, we also established that their relationships could group them at different abstraction levels. Because the connections in this graph are directed, the link's direction can be used as a property for sorting the graph. The grouping can be done by applying topological sort to the activities by their connections in space to either point up or connect laterally.

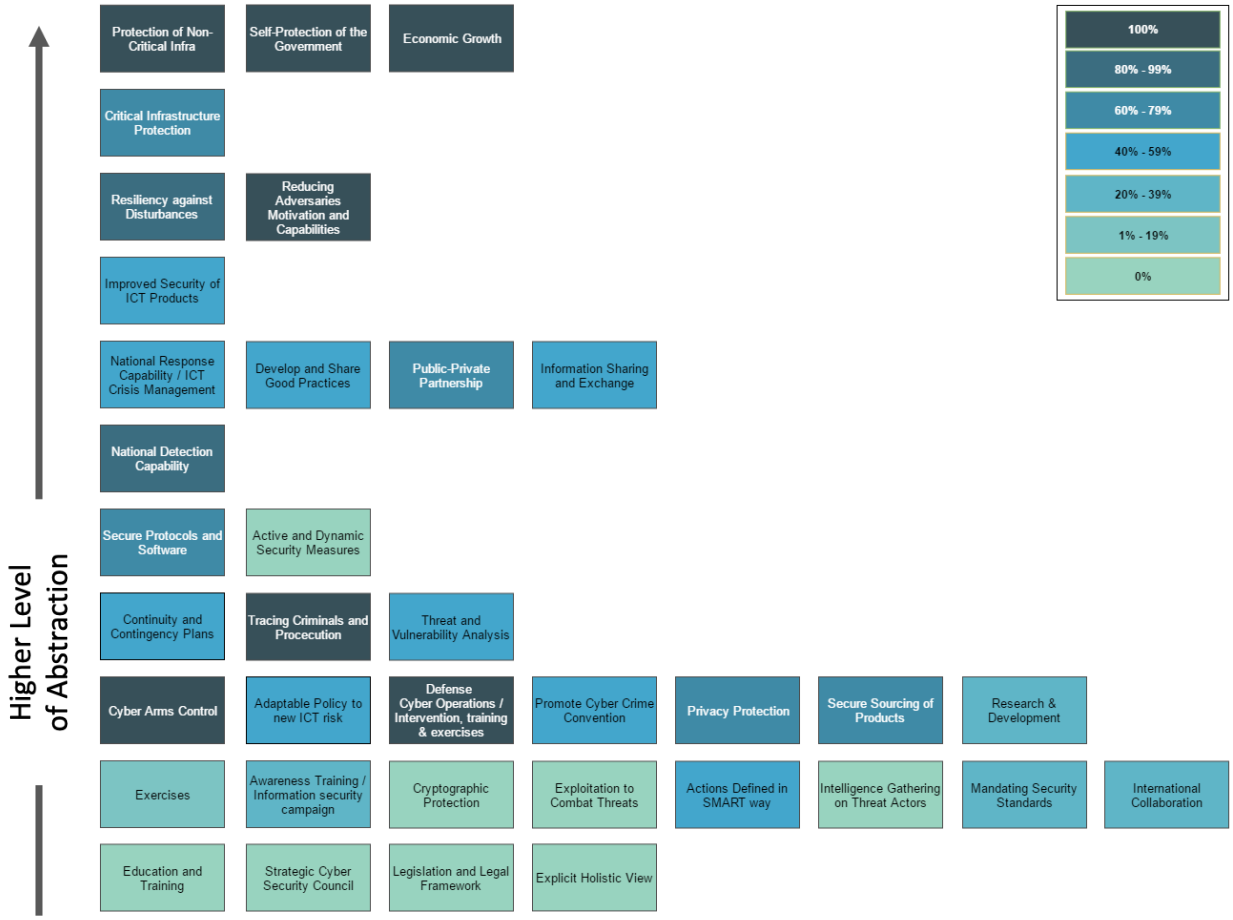


**Figure 3:** Activities sorted by causal relations

The activities can be projected into a line with only outbound relationships at one end and only inbound relationships at the other end. The majority of the activities are positioned somewhere in the middle of the line. However, once we identify which activities are at the top of the hierarchy and which ones are at the bottom, we can infer the approximate level of abstraction of these individual activities.

In Figure 3 above, the activities have been sorted by their inbound and outbound connections. There are only lateral links or links to a layer above. Some links cross multiple layers but always upwards in the diagram. The dark blue activities in this diagram only have links to them, never links from them to another activity. The lightest blue activities have no links to them, only links to other activities.

## 5.9 Verifying identified activities

The next step in drilling down into the activities would be to find out how accurately they have been detected in the original documents. Performing the cross-checking between the activity and the matching statement in the NCSS document would further clarify how rigorous the vetting of references was before adding to Luiijf's table. It would also provide insight into whether the research methodology of classifying the activities was sound, regardless of the poor fit when the results were compared to the Lithuanian NCSS document.

Detailed analysis of cross-checking all the listed activities from all the 19 separate NCSS documents is beyond the scope of this thesis, but tracking one of the less common activities in documents is a way to see some examples of the results. Having fewer occurrences would also mean that the activity must be fitted to cover a less generalized

case. In this kind of scenario, the activity should match more closely with the source document. If there are no matches, it will indicate that the activities may not have been appropriately captured.

Example: “Active/dynamic security measures” are listed as having been found in the NCSS documents for Estonia, India, Japan, and the USA, which provides a sample set for review analysis.

From the Estonian NCSS, the closest match to this activity would be the following statement: *“Civil, military, and international cooperation based on the resources at the disposal of the state must also function adequately in cyberspace – with regards to the warning, deterrence, and active defense.”* (Retel, 2014)

The exact phrasing of the activity does not appear to match well with the proposed activity. In India's case, no statement matching this activity could be found from the NCSS document in the review. It is not clear how the author arrived at their conclusion that the Indian NCSS mentions this activity. (Government of India, 2013)

In Japan’s NCSS document under the heading “Basic policy,” the author mentions the importance of *“Establishing active rather than passive information security measures.”* They continue to describe this in the following way: *“Conventional information security measures have tended to remain as symptomatic treatment that addresses individual risks whenever they arise, and often fail to address the actual cause. As ICT advances, information security measures that will 3 bring fundamental solutions to such problems must be strategically identified. At the same time, by utilizing the Plan-Do-Check-Act (PDCA) cycle and other methods, organizational structures that enable entities to actively implement new information security measures—differing from the current passive attitude—must be established.”* (NISC, 2010, p. 2)

This passage could be the origin of the activity that Luiijf calls “active/dynamic security measures” since it is the only one that uses the word “actively.” Although it is not as clearly spelled out in other Estonia and India documents, they were included under this header.

The lack of an exact source suggests that the authors have been creative and liberal in interpreting and selecting the activities and that the activities were not necessarily spelled out explicitly in the NCSS documents. For example, activity may describe the document's intention spread over paragraphs rather than in a clearly defined statement. If the selection criteria are not strictly applied, it is pretty challenging to prove that the authors of the NCSS document had that explicit motivation for each activity.

Establishing whether this is just a single incident of a low-quality match or an indicator of a general trend requires a more careful analysis of all the referenced documents.

# 6. Discussion

Several exciting topics arose during the research, and there are also new contributions to the research. The chosen research methods were successful to a degree, but there is still significant room for improvement. Significant limitations related to the prior research were also discovered, but those limitations also provide a helpful way to think about the results.

The driver for using the constructive analysis method to define the objectives and activities was the consistent inability to evaluate the research methods or reproduce any of the prior research in this domain. None of the previous research or publications documented in their methodology used to arrive at the result presented in the publication in sufficient detail.

In rigorous research, one should be able to do so by applying the same method, and this restriction sets boundaries on how reliable the source material can be. While this research into NCSS documents does not necessarily carry the same weight as other natural and social sciences where the problem of replicability is an actual crisis, the concern may extend here as well. The constructive analysis is a way to try to establish a reproducible method of analyzing the contents of NCSS documents; anyone can apply it and see if they get the same result as this work. It would be great to see future research in this field publish their methodology in full.

## 6.1 Understanding activities related to cybersecurity strategy

Understanding the causal relationship between the activities identified during the research for this thesis is a novel contribution that has not been seen in prior published research based on searches in the electronic journal databases. While the analysis was done within the limiting boundaries of the existing and partly aged source material, the discussed objectives and activities continue to be relevant today. All of the studied material was included in the NCSS evaluation frameworks research used as primary source material. A couple of valuable observations can be made from the results of the analyzed activities.

First, there is a division of activities into groups; some are prerequisites for multiple other activities and other activities that require supporting activities. The delineation is gradual, and the activities towards the top of the ranking hierarchy are more likely to be high-level objectives than activities. However, this may not be a meaningful metric since being activity or objective is based on the evaluation method used in this work. The classification depends on how many dependencies an activity has with other activities or how high the level of abstraction is. The status is probably not stable and is also likely to change as more relevant objectives and activities are introduced to the analysis.

Second, based on the analysis, it is prudent to propose that a more detailed understanding of dependencies in this kind of documents could be a significant resource for designing strategies. The knowledge of these links already exists in the expertise of the people who are familiar with this domain. For example, the objective “Improved security of ICT products” is dependent on the activity “Secure protocols and software.” Most people familiar with the cybersecurity domain would agree with this assertion and recognize the dependency direction between these activities. Many of the other links are not so obvious and only become apparent when the whole dependency graph is examined as a whole. Ferreting out and presenting these links describes our current understanding of this domain in a very compact representation.

Third, because NCSS documents are developed for a wide variety of audiences, from high-level decision-makers to those implementing individual activities, an objective for another is an activity for the other. Therefore, a resulting relationship diagram helpful to one user may not work for another and may include unnecessary detail. Therefore, the intended audience should be taken into account in future work.

## 6.2 Differences between Luiijf´s and Lithuanian document

We can safely say that the listed activities in Luiijf's work are unlikely to be a complete set. However, since no other sources could be found that would attempt to do a similar analysis, and the other primary sources did not claim to find the same activities, that assertion cannot be verified at this time. Furthermore, making that claim would require replicating the prior studies and reviewing all the currently available NCSS documents.

As a thought exercise, there are at least three likely sources of additional objectives and activities that would meaningfully contribute to this analysis:

1. The authors of the evaluation studies may not have reliably noted all the objectives and particularly the activities in the NCSS documents that they studied.
2. Suppose the original analysis studies would be extended into the rest of the available source material (NCSS documents from other countries). In that case, more activities that match the definition would likely be added to the list.
3. Many countries have published one or more new editions of their cybersecurity strategy since the prior research was published. Those new editions are likely sources of new activities or existing activities that have been further refined.

The existing NCSS documents also most likely do not contain all the relevant activities that would positively contribute to national cybersecurity. The development of the cybersecurity field both produces new insights and methods of improvement. More activities can and will be added as new countries develop their documents and produce new revisions of their respective NCSS documents.

## 6.3 Applicability of Kolini's LDA analysis

Even though all the member countries whom OECD investigated in their work are listed in Kolini's analysis, there is a five-year gap between the analyses. Therefore, it is possible that the understanding of the relevant cybersecurity topics in these countries may be different when Kolini's analysis was performed. It is also possible that the second version of an NCSS has been published during that time. However, it was not feasible to investigate which versions of the NCSS documents were included in Kolini's data set as they do not list the NCSS documents in the references. In addition, Kolini only mentions a summary of included countries rather than the actual documents in their article's data description section.

The second factor to consider is that the machine learning approach's outcome is challenging because we do not know what words, groupings, or clusters are left out from the results when the algorithm produces the desired number of clusters. Compared to human analysis, it is not straightforward to determine, for example, if some relevant clusters or topics make sense and are important, but where the content in the documents was spread so thinly that the algorithm did not catch it.

There is some evidence of this type of omission when evaluating the results. For example, Kolini's word clusters do not appear to produce a topic that could be labeled "economic

development," even though that topic or the underlying idea is present in most of the NCSS documents published. The economic factors are prominent enough in the NCSS documents that they have been studied, for example, by the NATO CCDCOE center (Brangetto and Kert-Saint Aubyn, 2014). Luiijf also made this observation in their analysis. (Luiijf et al., 2013, p. 11)

One of the LDA analysis parameters is the desired number of clusters that the output should have, significantly affecting the results. Kolini and Janczewski settled on ten clusters in their work after studying the experiments' results with 5, 10, 15, 20, 50, and 100 clusters. The optimal number of topics for a particular context depends on the size and variability of the source corpus and the analyst's subjective interpretation. It is difficult to say definitively whether a better result would be achieved using, for example, 8 or 12 clusters instead of 10. These clusters can be considered topics for our purposes after being classified and named by the researchers. It is always up to the human analyst to assign a meaningful label encompassing the list's terms. The algorithm is unable to define the topic that the cluster represents on its own.

The second apparent omission is the lack of category that could be labeled "Intelligence gathering and sharing," represented by activities #16 and #17 in Luiijf's list. In the 19 NCSS documents, activity #16 is mentioned in 11, and activity #17 in 7 documents. We can extrapolate that the activities should exist in 33 to 50 percent of the more extensive selection of documents that Kolini analyzed. Nevertheless, Kolini's approach does not lift this cluster as part of the ten proposed clusters. It appears unlikely that the source of the difference is that the 41 additional NCSS documents analyzed had suddenly stopped including intelligence gathering as an activity. That would need to be verified by reviewing the entire 60 NCSS document source material to see if that topic can be found.

The inability to produce this category in the results is a significant drawback for the analysis method. Those clusters could appear if the algorithm were directed to produce, for example, a set of 15 clusters. Determining the optimum number of clusters by an algorithm is also subject to ongoing research. Heuristic approaches that produce a stable result could have been applied to the evaluated study. Such methods have already been proposed and tested. (Zhao et al., 2015)

## 6.4 Standardization of an NCSS document

Studying the analyses and the NCSS documents published by countries makes it clear that there is no standardized way of defining a national cybersecurity strategy. Instead, each country develops its own. While many of them have done extensive research on documents released by other countries, each document is unique in both format and content. They draw influence from documents published by other countries and draw some language from previously published documents, as shown in Kolini's research about NCSS document "family tree." (Kolini & Janczewski, 2017.)

It would be beneficial for the NCSS documents to spell out the dependencies between the activities and objectivities for the standardization of objectives and activities. Explaining the requirements was partly done in the Lithuanian strategy, but it is not a common practice.

It remains to be seen whether the cybersecurity strategy "Capability Maturity Model for Nations" made by GCSCC will significantly impact national strategies' harmonization. ENISA's work on providing additional guidance on writing NCSS documents may also have harmonizing effect over time, particularly in European countries. The influence of

their guidelines could be researched by studying the evolution of the future NCSS documents. One way to analyze the impact would be applying Kolini's document hierarchy classification scheme for documents published more than one year after the model was published or by surveying the authors of the more recent documents on which frameworks influenced their process.

It would be beneficial if a standard method of defining the document could be adopted to be more comfortable for countries to review their strategies in the context of other countries' strategies. This kind of standardization may evolve and can be a realistic prospect. The documents are meant to be adapted to the countries' changing requirements and generally designed to be updated roughly every five years, so there is ample space for finding common approaches.

## 6.5 Validity

Thorough validation of the extent to which the NCSS documents were intended to describe activities would have required extensive additional study of the national strategies. In addition, the validation would be challenging to accomplish with the available resources because the implementation plans are not necessarily translated to English. Usually, only the strategy document itself is translated as implementation is only for local interest.

For this study's purposes, it did not significantly impact since source material claimed to have extracted many activities from the documents. Nevertheless, there was also source material in the NCSS documents that did define activities, so the starting point was valid.

Since none of the studies providing the source material describe how they arrived at their definitions, it is impossible to directly assess the quality of those definitions used for identifying activities for the studies. The lack of visibility brings ambiguities to the analyses performed in this research. However, it did not make it impossible to perform the analyses needed to answer the research questions.

One problem in accomplishing activity definition in practice is that the activities' descriptions are too truncated, often reduced to the minimum amount of words necessary to convey the intent. However, being so brief, it is often too short for the reader to have confidence in the meaning.

There could be many reasons for this conciseness: authors preferred concise terms or wanted to fit them neatly into a table in the publication. Thus, it would likely be possible to extract more verbose descriptions by going back to the source publications. However, given the constraints, it would be impossible to replicate the results as the material and research method have not been disclosed for any source analyses. Therefore, future research into these topics should carefully disclose the methodologies used for content extraction and analysis so that there is enough transparency to evaluate the work. In this thesis, all the content used for analysis comes from primary sources and continues to be publicly accessible.

# 7. Conclusions

This thesis set out the study the methods and frameworks previously used to analyze national cybersecurity documents. NCSS documents have a general goal of improving society's cyber resilience and making sure that technology can be leveraged to its full potential to advance the economy in an environment full of risks.

Since the documents are built around a central theme and ostensibly have the same goal, they should be similar in theory. That implies that review frameworks should have no trouble finding similarities among the NCSS documents.

Analysis of the results showed that was not the case. The results of previous analyses were not easily comparable and approached the research from very different perspectives. Previous frameworks were opaque in the research methodology on how they selected objectives and activities from the source material and produced inconsistent results that proved difficult to replicate by looking at the source material. The activities and objectives extracted from the documents in separate analyses did not correspond to each other. Perhaps more alarmingly, they did not always even correspond with the source material in the sampled cybersecurity documents mentioned as sources.

Performing a deeper analysis of the extracted activities from the documents enabled the extraction and examination of relationships between them. One of the research questions was about figuring out how the activities relate to each other. The work on that produced the activity graph and the resulting hierarchical arrangement of the activities by their abstraction level. Understanding the hierarchy and relations becomes much more concrete when described in this kind of graphical representation. That is a valuable finding because there has not been published research into these activities since 2013. Kolini's work from 2017 is the only exception, but the research approach is so different that it does not extend the earlier work, rather than providing another perspective. Meanwhile, up to a hundred national strategies have been published globally, affecting both policies at the very center of cybersecurity preparedness and resiliency.

The resulting information about the activities and objectives' dependencies could be helpful when designing new implementation plans for cybersecurity strategies. The knowledge base from the graph produced in this research could be used for multiple purposes. For example, it is essential to know that the proposed objectives and activities are reasonable and that all the prerequisites are known before the publication of a strategy. Otherwise, the publisher is at risk of including impossible objectives because of a lack of knowledge, organizations, policies, training, or other prerequisites. In that scenario, it makes more sense to set less ambitious goals or document that achieving the prerequisite goals is needed to achieve the overarching goal stated in the document. It also makes more sense to emphasize the achievable but essential objectives.

A shared body of knowledge about objectives and proposed activities in cybersecurity strategies would be helpful. It makes little sense that these are objectives are developed from scratch or by taking another country's document as a base and then customizing it to the situation, which seems to happen according to the family tree of NCSS documents as shown by Kolini. A general framework would be more effective, cover more situations, and provide neutral guidance to the practitioners, who could then choose to include the parts they need. The work that began in this thesis could contribute to that by providing a seed for the objectives and activities commonly present in NCSS. In addition, should

that work compile the knowledge base from scratch, the constructive analysis method could start working out the relationships from a larger corpus of the source material.

Knowing which activities depend on each other could also influence policy decisions on what activities should be defined in a strategy. Unfortunately, the writing of these strategies currently relies on the expertise of the individual contributors that typically write them in committees. While they are likely to have tremendous personal experience in cybersecurity and their particular fields, cybersecurity as a domain is vast. No single person can grasp all of it and be aware of all the dependencies and relationships necessary to advance particular agendas.

For example, suppose that an objective cannot be achieved in the expected lifetime of the strategy because there are intermediate steps that depend on other capabilities. It does not make sense to include that as an objective in the strategy rather than adding the intermediate goals that will later lead to the desired state. Moreover, those intermediate steps should be documented so that those who implement the strategy can take them into account in their implementation plans.

While relationship graphs are not new, the ones produced in this work appear to be novel to a cybersecurity strategy. The graph linking the activities to each other and labeling the activities into three groups can inform the developer of the strategy's objectives and priorities. The benefit for the reader is getting a quick overview without having to read through large amounts of other countries' strategies and synthesizing the knowledge for themselves.

The guidance available from frameworks such as the Capacity Maturity Model for Nations produced by GCSCC is helpful. However, its contribution is to list a set of dimensions and aspects of those that can be measured objectively. Measurement in these dimensions leads to aspiration to improve on the areas, but there is little guidance on defining objectives and actions to progress cybersecurity to the desired level. That would be the content in the NCSS documents, especially in the implementation plans of those strategies, but there are few publications in this area.

## 7.1 Future research – Extensive activity and objective mapping

The produced graphs could be enhanced in several different ways. First, the activities were sourced from the source research done in 2013 and only included 19 NCSS documents as a source. Now that more than a hundred NCSS have been published and up to three iterative revisions for certain countries' strategies, a wealth of new source material could be mined for more content and improve the results.

In this thesis, mapping was performed for activities and objects collected from the existing analyses performed for a subset of NCSS documents available at that time. That knowledge graph can already be analyzed for insights. However, it could be significantly expanded if it considered all the activities and objectives present in a current generation of about one hundred NCSS documents. These kinds of links can be discovered in multiple ways. One such way would have been reading through the source material and identifying when activity or objective has explicitly stated dependencies. That could be done for all or for a subset of currently existing NCSS documents, which would create a knowledge base of consensus-based opinion on these dependencies.

The knowledge graph could also be used when evaluating NCSS documents from the perspective of understanding gaps in the implementation plan. The implementation plan needs to take into account what are the prerequisites for achieving the strategic objectives.

## 7.2 Future research - Generational document analysis

The number and corpus of second and third-generation NCSS documents released by countries already enable generational difference analysis of the released documents. The analysis could be done using Kolini's LDA method and comparing the resulting categories produced by the algorithm. One could also perform manual analysis for documents sorted by generation using the document review method such as the one used by Luiijf.

It would also be fascinating to see the results of new research of topic modeling that would include all the currently existing 104 documents. That would then also provide the complete cluster data sets for a range of 10-20 clusters. In this way, one could analyze the produced clusters more thoroughly and determine the topics in more detail.

Another interesting approach would be performing an analysis where NCSS documents are bucketed in time-based generations, such as five years each. One could then compare those NCSS documents released between 2007-2011 with the strategies released in the 2012-2016 and 2017-2021 time periods. Results of both framework-based and machine learning-based analyses would provide insight into this domain's general development. It could expose how different prominent topics are between the document generations and how common it is to find those topics in that generation's NCSS documents. Currently, there is very little research on how NCSS documents evolve, how the objectives defined in them evolve, whether some of those objectives are more successful than others, or if actions designed to reach those objectives are functional or not. Research and documentation of these areas would provide fascinating insights and assist nations in a significant way of choosing and plotting their path by developing the national cybersecurity strategy.

One aspect of whether an activity is well defined depends on the perspective of the audience. There may be different perspectives that exist at different levels of the government, between the private and public sector, or industries, and so on. Additional insight into the proposed activities' quality could be gained if the proposed activities would be studied from different perspectives and quantified on whether it adequately describes a relevant activity. The perspective-based analyses would quickly form another research project in its own right.

This topic is fascinating and could be significantly expanded by further analysis into the activities discovered in the national documents that were not available when Luiijf's second expanded analysis was performed in 2013. Discovering all of the proposed activities and the causal relationships of the activities in the complete corpus of NCSS documents available now would provide significant insight into which activities or groups of activities should be included in the NCSS documents under development. In addition, it would assist in the NCSS design and drafting process by providing the author ways to compare their proposed activities with the strategy's improvement goals and the current state of the matters in their countries.

The LDA-based machine-learning approach lays the foundation for this. It can already build a ”family tree” of related NCSS documents, which may tell what existing documents were used as inspiration when writing the strategy. Kolini demonstrated that

the research was not verified by interviewing the authors to discover if those associations were just artifacts of their topic modeling methodology. It would have been a significant verification of the automated research into this topic. Unfortunately, that research into the currently available documents was outside of this thesis's scope.

# 8. References


Azmi, R., Tibben, W., & Khin, T. W. (2016). *Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy.* Wollongong.

Bernat, L., Ford, P., & Mansfield, N. (2012). *Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy.* Organization for Economic Co-operation and Development (OECD). Retrieved from http://oe.cd/cybersecurity-strategies

Brangetto, P., & Kert-Saint Aubyn, M. (2014). Economic aspects of national cyber security strategies. Tallinn, Estonia.

Brangetto, P., & Veenendaal, M. A. (2016). *Influence Cyber Operation: The Use of cyber attacks in support of influence operations.* Tallinn: NATO CCD COE Publications.

Ellefsen, I. (2014). The Development of a Cyber Security Policy in Developing Regions and the Impact on Stakeholders. *IST-Africa 2014.* Johannesburg.

Enescu, S. (2020). A Comparative Study on European Cyber Security Strategies. *Redefining Community in Intercultural Context*, *2020/01*, pp. 277-282. Cluj-Napoca.

Falessi, N., Gavrila, R., Klejnstrup, M. R., & Moulinos, K. (2012). *National Cyber Security Strategies - Practical Guide on Development and Execution.* Heraklion, Greece: European Union Agency for Network and Information Security.

Global Cyber Security Capacity Centre. (2016). Cyber Security Capability Maturity Model for Nations (CMM). Oxford: Oxford University.

Government of Finland. (2013). *Finland´s Cyber security Strategy.* Ministry of Defense, Secretariat of the Security and Defence Committee, Helsinki.

Government of Finland. (2016). *Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020.* Ministry of Defense, Secretariat of the Security Committee, Helsinki.

Government of Finland. (2019). *Finland's Cyber Security Strategy 2019.* Ministry of Defense, Secretariat of the Security Committee, Helsinki.

Government of India - Ministry of Communication and Information Technology. (2013, July 2). *Notification on National Cyber Security Policy - 2013 (NCSP-2013).* Retrieved from https://www.cert-in.org.in/ISAC-Power/National_Cyber_Security_Policy_2013.pdf

Government of Ireland. (2014). *National Cyber Security Strategy: Securing our Digital Future.* Department of Communications, Energy and Natural Resources. Dublin: Government of Ireland.

Government of Lithuania. (2011). *The programme for the development of electronic information security (cyber-security) for 2011-2019.* Government of Lithuania.

International Telecommunications Union. (2018). *Guide to Developing a National Cybersecurity Strategy – Strategic engagement in cybersecurity.* ITU.

International Telecommunications Union. (2019, 05 23). *Study Group 17 / Cyber Security*. Retrieved from International Telecommunications Union: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Kolini, F., & Janczewski, L. (2017). Clustering and Topic Modelling: A New Approach for Analysis of National Cyber Security Strategies. *PACIS* (p. 13). Association for Information Systems.

Kosterec, M. (2016). Methods of conceptual analysis. *Filozofia*(3), 220-230.

Lehto, M. (2013). The Ways, Means and Ends in Cyber Security Strategies. *The Proceedings of the 12th European conference on information warfare and security* (pp. 182-190). Jyväskylä: Academic Publishing.

Luiijf, E. (2019). *National Cyber Security Strategies*. Retrieved 15.2.2021, from CIPedia.eu: https://publicwiki-01.fraunhofer.de/CIPedia/index.php/National_Cyber_Security_Strategy

Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure Protection*, 31. doi:10.1504/IJCIS.2013.051608

Luiijf, H. A., Besseling, K., Spoelstra, M., & de Graaf, P. (2011). Ten national cyber security strategies: A comparison. In *Critical Information Infrastructure Security* (Vol. 6983, pp. 1-17). Springer Berlin Heidelberg. doi:10.1007/978-3-642-41476-3_1

Min, K.-S., Chai, S.-W., & Han, M. (2015). An International Comparative Study on Cyber Security Strategy. *International Journal of Security and Its Applications, 9*(2), 13-20. doi:10.14257/ijsia.2015.9.2.02

Network Security. (2016). UK Government launches new £1.9bn cyber-security strategy. *Network Security*(11), 1-2.

NISC. (2010). Retrieved from National center of incident readiness and strategy for cybersecurity (NISC): https://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf

Republic of South Africa. (2010). *Draft Cybersecurity Policy of South Africa.* Pretoria: Department of Communications, Republic of South Africa.

Retel, S. (2014). *Estonian Cyber Security Strategy 2014-2017.* Tallinn: Estonian Ministry of Economic Affairs and Communications. Retrieved 06.01.2016, from European Union Agency for Network and Information Security: https://www.mkm.ee/en/objectives-activities/information-society/cyber-security

Robinson, N., Horvath, V., van der Meulen, N., Harte, E., & van der Sar, M. (2014). *An evaluation Framework for National Cyber Security Strategies.* (D. Liveri, & A. Sarri, Eds.) Heraklion, Greece: European Union Agency for Network and Information Security. doi:10.2824/3903

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards more representative definition of cyber security. *The Journal of Digital Forensics, Security and Law, 12*(2), 53-74.

Shafqat, N., & Massod, A. (2016). Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security, 14*(1), 129-136.

Štitilis, D., Pakutinskas, P., & Malinauskate, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: A comparative analysis. *Security journal, 30*(4), 1151-1168.

Štitilis, D., Pakutinskas, P., Laurinaitis, M., & Malinauskaitė-van de Castel, I. (2017). A model for the national cyber security strategy. The Lithuanian case. *Journal of Security and Sustainability Issues*, 357-372.

Teoh, C. S., & Ahmad, K. M. (2017). National cyber security strategies for digital economy. *Journal of theoretical and applied information technology, 95*(23), 6510-6522.

The Open Web Application Security Project. (8.2.2021). *OWASP Top 10*. Retrieved from The Open Web Application Security Project: https://owasp.org/www-project-top-ten/

Van Solingen, R. &. (1999). *The Goal/Question/Metric Method: a practical guide for quality improvement of software development.* McGraw-Hill.

Von Solms, R., & van Niekerk, J. (2013). *From information security to cyber security.* Port Elizabeth: Elsevier.

Von Wright, G. H. (1963, April). Practical Inference. *The Philosophical Review, 72*, 159-179.

Woody, C., & Ellison, R. (2020). *Building a Cybersecurity Strategy.* Systemics, Cybernetics and Informatics.

Zhao, W., Chen, J. J., Perkins, R., Liu, Z., Ding, Y., & Zou, W. (2015). *A heuristic approach to determine an appropriate number of topics in topic modeling.* BMC Bioinformatics.